SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2004–2005

An Operational Review of the
Canadian Security Intelligence Service

Canada

Security Intelligence Review Committee
P.O. Box 2430, Station "D"
Ottawa ON
K1P 5W5

Tel: (613) 990-8441
Fax: (613) 990-5230
Website: http://www.sirc-csars.gc.ca
Collect calls are accepted between 8:00 a.m. and 5:00 p.m. Eastern Standard Time.
© Public Works and Government Services Canada 2005
Cat. No. PS105-2005
ISBN 0-662-69304-3

SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2004–2005

An Operational Review of the Canadian Security Intelligence Service

Canada

September 30, 2005

The Honourable Anne McLellan, P.C., M.P.
Deputy Prime Minister and
Minister of Public Safety and Emergency Preparedness
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

As required by Section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2004–2005, for your submission to Parliament.

Yours sincerely,

Gary Filmon, P.C., O.M.
Chair

Baljit S. Chadha, P.C.

Roy Romanow, P.C., O.C., Q.C.

Raymond Speaker, P.C., O.C.

M[me] Aldéa Landry, P.C., Q.C.

Contents

Statement from the Committee vii

About this Report ix
How this Report is Organized ix
Identifying SIRC Studies: Choices and Challenges x

Section 1: A Year in Review 2004–2005 1

A. Reviews of CSIS Security Intelligence Activities 3
Overview: How SIRC Carries Out its Review Function 3
The Committee's Role in CSIS's Accountability Structure 3
SIRC Reviews in 2004–2005 4
Review of the Terrorist Entity Listing Process 4
Review of CSIS's Investigation of Transnational Criminal Activity 10
Review of a Counter-Terrorism Investigation 14
Review of Activities and Investigations in a CSIS Regional Office 17
Review of a Counter-Proliferation Investigation 20
Review of CSIS's Information Operations Centre 21
Review of CSIS's Exchanges of Information with Close Allies 23
Review of a Counter-Intelligence Investigation 26
Terrorist Financing Activities in Canada 28
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post 31
Review of Foreign Arrangements 33

B. Investigation of Complaints 36
Reports of Decisions: Case Histories 38
Human Rights Complaint Referral 38
Report: Section 41 ("Any Act or Thing") 39
Report: Section 42 (Denial of Security Clearance) 39

C. Section 54 Report to the Minister of Public Safety and Emergency Preparedness 41

Section 2: CSIS Accountability Mechanisms 43

A. Reporting Requirements 45
Certificate of the Inspector General for 2004 45

CSIS Director's Annual Operational Report 2003–2004 46
Unlawful Conduct by CSIS 49
Section 2(d) Investigations 49
Disclosures of Information in the Public or National Interest 49

B. Policy and Governance Framework 50
Annual National Requirements for Security Intelligence 50
Ministerial Direction 53
Governor-in-Council Regulations and Appointments 53
Changes in CSIS Operational Policy 53

C. CSIS Operational Activities 54
Counter Proliferation 54
Counter Terrorism 55
Counter Intelligence 56
Research, Analysis and Production (RAP) Branch 56
Security Screening 58
CSIS Domestic Arrangements 66
Federal Court Warrants and Warrant Statistics 67

Section 3: Want to Know More? An Overview of SIRC 71
Committee Membership 73
Staffing and Organization 73
Research and Review Activities 73
Security Intelligence Briefings 74
Additional Committee Activities 74
Budget and Expenditures 75
Inquiries Under the Access to Information and Privacy Acts 76
Modern Comptrollership 76

Appendix A: Acronyms 77

Appendix B: SIRC Reports and Studies Since 1984 81

Appendix C: Key Findings and Recommendations 93
Review of the Terrorist Entity Listing Process 95
Review of CSIS's Investigation of Transnational Criminal Activity 95
Review of a Counter-Terrorism Investigation 96
Review of Activities and Investigations in a CSIS Regional Office 96
Review of a Counter-Proliferation Investigation 97
Review of CSIS's Information Operations Centre 97
Review of CSIS's Exchanges of Information with Close Allies 98
Review of a Counter-Intelligence Investigation 99
Terrorist Financing Activities in Canada 100
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post . 100
Review of Foreign Arrangements 101

106-02582/

Statement from the Committee

Twenty Years After the Establishment of the *CSIS Act*, Security Intelligence in Canada Faces New Challenges

Twenty years have passed since both the Security Intelligence Review Committee (SIRC) and the Canadian Security Intelligence Service (CSIS) came into being. Looking back over the span of those two decades, it would be an understatement to say that much has changed in the domain of national and global security. Yet what cannot be overstated is how much of that change has taken place just within the last five years. In Canada and around the world, many security intelligence services have had to evolve quickly from being primarily counter-intelligence organizations into ones whose main focus is combatting terrorism domestically and abroad.

The pace of this evolution gained momentum in 2001, immediately following the September 11th terrorist attacks, as Canadians saw the emergence of new measures in the form of the *Anti-Terrorism Act*. Today, information gathering and assessment activities are spread out among a number of federal organizations, with the result that the security intelligence environment is both more complex and more integrated. This has important ramifications for citizens and for policy-makers—after all, SIRC's raison d'être has been to provide a balance against the potent, intrusive powers conferred upon CSIS by the *CSIS Act*. Similar powers are now being exercised by other public bodies, some without the same level of scrutiny that SIRC imposes on CSIS.

SIRC applauds the government's commitment to achieve an effective integration of its operational intelligence apparatus. SIRC also endorses the logical next step, which is a comprehensive and more integrated review of that apparatus. As do many Canadians, we look forward to the findings of Mr. Justice Dennis O'Connor, whose policy review is charged with making recommendations for a review mechanism for the RCMP's national security activities.

The *Anti-Terrorism Act* not only supports Canada's domestic efforts to combat terrorism, but also has an important international dimension—that of harmonizing Canada's anti-terrorism laws with those of its global partners. It is this dimension that has broadened the limits of CSIS's intelligence collection efforts and has tested SIRC's ability to conduct a complete review of the Service's activities.

Indeed, for the first time in many years, SIRC finds itself in the unhappy position of not being able to review comprehensively certain activities by the Service—responsibilities that have been conferred on CSIS by the *Criminal Code*, as amended by the *Anti-Terrorism Act* (this issue is explored at length in this annual report on page 4). Although these activities represent a relatively small slice of CSIS's work, they have significant potential to affect individuals negatively.

To be clear, this is a matter not of CSIS's making. Nevertheless, this Committee believes it is of paramount importance that all of CSIS's activities, including any extension thereof, be subject to independent scrutiny. After all, the *CSIS Act* was passed by Parliament so that the Service's significant powers would be clearly defined and kept in check.

We believe it is important, therefore, that Parliament ensure that the laws governing review keep pace with legislative initiatives in support of intelligence capacity. Such vigilance will help avoid creating a vacuum in the area of security intelligence review.

Indeed, much has changed since 1984, but the framework that defines the powers and authority of both CSIS and SIRC is one that has stood the test of time. The past twenty years have seen both SIRC and CSIS evolve to meet the challenges of security intelligence in Canada, while building a legacy of commitment to rights and the rule of law. We look forward to playing a continuing vital role in Canada's security intelligence community in the years ahead.

About this Report

How this Report is Organized

The Security Intelligence Review Committee exists to provide assurance to the Parliament of Canada—and through it, to Canadians—that CSIS is complying with law, policy and Ministerial Direction in the performance of its duties and functions. SIRC has two key functions. The first is to conduct in-depth reviews of CSIS activities to ensure that they comply with the *CSIS Act* and the various policy instruments that flow from it, and with direction from the Minister of Public Safety and Emergency Preparedness. The second is to receive and investigate complaints by any person about any action of the Service.

The 2004–2005 annual report is organized to reflect the Committee's key findings. Additional information that the Committee believes will provide useful background, historical or technical information is set apart from the main text in shaded insets. These insets are intended to be factual and do not reflect Committee opinions or conclusions.

As with previous annual reports, the format of this publication distinguishes between Committee findings, observations and recommendations arising from in-depth reviews or complaints investigations, and more general background material collected to inform Committee Members and assist readers in understanding the broader context in which CSIS's security intelligence work is carried out.

Section 1: A Year in Review 2004–2005
This section provides the reader with summaries of the eleven major reviews SIRC conducted during the period covered by this report. In addition, it provides information regarding complaints received by the Committee. Finally, this section summarizes a special report forwarded to the Minister of Public Safety and Emergency Preparedness in accordance with Section 54 of the *CSIS Act*.

How this report is organized *(continued)*

Section 2: CSIS Accountability Mechanisms

Featured in this section are descriptions of the policy and governance framework within which CSIS carries out its duties and functions. This section also outlines information provided to SIRC by the Service relating to their branch investigations and changes to CSIS operational plans and priorities.

Section 3: Want to Know More? An Overview of SIRC

This section provides details of the information gathering, outreach, liaison and administrative activities of the Committee, including SIRC's annual budget and expenditures.

Identifying SIRC Studies: Choices and Challenges

SIRC's research program is designed to address a broad range of subjects. In selecting these for review, the Committee takes into consideration:

- the scope of CSIS investigations;
- particular activities that could intrude on individual rights and freedoms, as well as priorities and concerns for Parliament and the Canadian people;
- the CSIS Director's classified report to the Minister on operational activities; and
- the importance of producing regular assessments of each of the Service's operational branches, and regional offices.

The Committee also considers a number of other factors when it approves specific areas for review:

- the Committee's statutory obligations as detailed in the *CSIS Act*;
- events with the potential to cause threats to the security of Canada;
- issues or concerns identified in previous Committee reports;
- commitments by the Committee to re-examine specific matters;
- issues identified in the course of the Committee's complaints functions; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows the Committee to manage the inherent risk of being able to review only a small percentage of CSIS activities in any given year. However, SIRC is always prepared to adjust planned activities to respond to unforeseen events. One such special review was prepared in the period covered by this report. Also noteworthy, SIRC was able to expand its research program in 2004–2005, as a result of new resources received through Supplementary Estimates.

Each review produced by the Committee follows a detailed examination of CSIS documents, interviews with Service staff and senior managers, and an assessment of the Service's actions in relation to applicable laws, policies and Ministerial Direction.

While SIRC has only a small team of researchers, it seeks to examine as broad a spectrum of CSIS's duties and functions as is possible. Over a period of years, the body of completed research projects has provided Parliament, and the Canadian public, with a comprehensive description and assessment of the Service's operational activities.

Section 1

A Year in Review 2004–2005

A Year in Review 2004–2005

A. Reviews of CSIS Security Intelligence Activities

Overview: How SIRC Carries Out its Review Function

THE COMMITTEE'S ROLE IN CSIS'S ACCOUNTABILITY STRUCTURE

The Security Intelligence Review Committee is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. The Committee was established under the *CSIS Act* (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is complying with law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, the Committee seeks to ensure that the fundamental rights and freedoms of Canadians are respected.

To fulfill its mandate, the Committee directs staff to undertake a number of review projects each year. These reviews provide a retrospective examination and assessment of specific CSIS investigations and functions. SIRC has virtually unlimited power to review CSIS's performance of its duties and functions. With the sole exception of Cabinet confidences, SIRC has the absolute authority to examine all information concerning CSIS's activities, no matter how highly classified that information may be.

Each review includes the Committee's findings and recommendations. Upon completion, the report is forwarded to the Director of CSIS and the Inspector General (IG), CSIS.

SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety and Emergency Preparedness on any matter that Committee Members identify as having special importance.

This review function enables the Committee to inform Parliament and the Canadian public on the activities of CSIS and to assess whether the Service's actions were carried out in accordance with the laws of Canada, directions from the Minister, and CSIS operational policy.

The Committee is but one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the existing apparatus of government, specifically the Minister of Public Safety and Emergency Preparedness, the Inspector General of CSIS, central agencies of the federal government, the Auditor General, the Information Commissioner, and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2004–2005

Review of the Terrorist Entity Listing Process

Report # 2004-03

In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*, specifically the Service's role in the Terrorist Entity Listing (TEL)[1] process.

The Committee's review identified two key issues:

In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*.

- the authority under which CSIS collects information for the TEL process, and the extent of their collection activity; and
- the constraints on SIRC's ability to reasonably undertake a review of the listing process.

CSIS's Authority for Engaging in the Listing Process

The TEL process is mandated under Section 83.05 of the *Criminal Code*, as amended by the *Anti-Terrorism Act*. CSIS's role in the TEL process is the creation of Security Intelligence Reports (or SIRs), considered by the Minister of Public Safety and Emergency Preparedness in her recommendation to the Governor-in-Council concerning whether or not an entity should be listed.

When examining the Service's role in the TEL process, SIRC asked:

- *What is the Service's authority to participate in the TEL process?;*
- *What is the meaning of "threats to the security of Canada," as defined in Section 2 of the* CSIS Act*?; and*
- *Is the definition of "threats to the security of Canada" in the* CSIS Act *consistent with the definition of "terrorist activity" in the* Criminal Code*?*

These questions were necessary because there are several entities on the *Criminal Code* list (which included 35 groups as of March 31, 2005) that do not appear to fall within the definition of "threats to the security of Canada" under the *CSIS Act*. For example, Japan's Aum Shinrikyo cult and Colombia's Autodefensas Unidas de Colombia are each listed as terrorist entities, but neither organization has committed a terrorist act on Canadian soil, nor does either have any obvious presence or support apparatus in Canada.

1. The *Criminal Code* refers only to a "list of entities." The acronym TEL is employed strictly to assist readers.

Section 2 of the *CSIS Act* is very specific, owing to the importance Parliament has placed on clear, legislative boundaries to the Service's collection activities. The *CSIS Act* defines "threats to the security of Canada" as activities "against Canada," or "detrimental to the interests of Canada" (2a); activities "within or relating to Canada" (2b, 2c); or activities "directed toward undermining" the "established system of

More about the Terrorist Entity Listing Process in Canada

In Canada, there are two mechanisms for being listed as a terrorist through domestic legislation: via the *United Nations Suppression of Terrorism Regulations* (UNSTR) or through the federal *Criminal Code* as amended by the *Anti-Terrorism Act*.

A person or group is placed on the UNSTR list if the United Nations Security Council agrees to list an individual or entity pursuant to the UN Afghanistan Regulations, which permits the listing of individuals or groups associated with the Taliban or Osama Bin Laden. As a UN member nation, Canada automatically adopts the listing. Alternately, a person or group may be placed on Canada's UNSTR list based on a recommendation by Foreign Affairs Canada (FAC). Usually this process begins when FAC receives notification of another country's intention to list a terrorist entity. FAC convenes an interdepartmental meeting to discuss the proposed listing and provides its recommendation to the Governor-in-Council. There are currently more than 480 names on the UNSTR list.

The names put forward for consideration for listing in the *Criminal Code* process emerge from interdepartmental consultation within the Government of Canada. Once an entity is suggested, the Service prepares a Security Intelligence Report (SIR) on that entity. The SIR is considered by the Minister of Public Safety and Emergency Preparedness, who makes a recommendation to the Governor-in-Council concerning whether or not the entity should be listed. There are almost 40 names on this list.

The consequences of being listed are serious. Anyone convicted of dealing directly or indirectly in property owned or controlled on behalf of a terrorist organization is liable to a fine of up to $100,000 and up to ten years in prison. The Office of the Superintendent of Financial Institutions (OSFI) maintains an entity list on its website (www.osfi-bsif.gc.ca) that includes all individuals and entities listed on both the *Criminal Code* and the UNSTR lists. Financial institutions are required to review their records on a continuing basis for names of persons on this combined list and to report immediately their findings to both the RCMP and CSIS.

government in Canada" (2d). Canada and Canadian interests are the common denominator in all four definitions of "threats to the security of Canada."

In contrast, Section 83.01 of the *Criminal Code* defines "terrorist activity" as an "act or omission," corresponding to the listed offences, that is committed "in or outside Canada." While the *CSIS Act* specifies a particular relationship to Canada (i.e., "within or relating to Canada"), the *Criminal Code* definition for terrorist activity may or may not relate to Canada, because it includes activities that may take place "outside Canada," and that need not specifically relate to Canada. It is not necessary for a terrorist activity to have a clear relationship to Canada for it to meet the definition of "terrorist activity" as defined by the *Criminal Code*.

The *Anti-Terrorism Act* was designed to harmonize Canadian legislation with that of its international partners. But this international dimension of the listing process is not accounted for in the *CSIS Act*.

As the Department of Justice has noted, the *Anti-Terrorism Act* was designed to harmonize Canadian legislation with that of its international partners.[2] But as a result of SIRC's review, the Committee noted that this international dimension of the listing process is not accounted for in the *CSIS Act*, which was designed to limit the Service's collection activity to national concerns.

What this Means from SIRC's Perspective

The Committee contends that the listing process may require CSIS to collect, retain, and analyze information that does not fall within the definition of "threats to the security of Canada" as defined in the *CSIS Act*.

As an analogy, CSIS's authority for investigating threats falls within two concentric circles. The inner, smaller, circle represents the Service's activity authorized under Section 12, which is limited to "threats to the security of Canada." The outer, somewhat larger, circle represents the Service's collection, analysis, retention and advice concerning information and intelligence on "terrorist activity" for the TEL process as mandated under the *Criminal Code*.

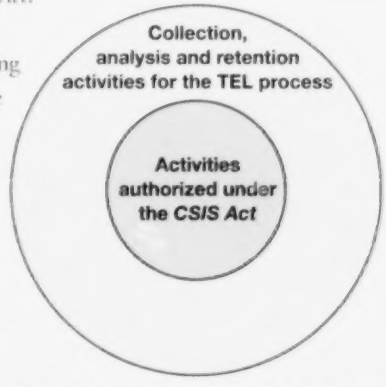

Figure: CSIS's investigative activity falls within two concentric circles

2. See Department of Justice fact sheet "Canada's Proposed *Anti-Terrorism Act*: Working with our International Partners" http://www.canada.justice.gc.ca/en/news/nr/2001/doc_27791.html (last updated April 24, 2003).

Much of the information in the two circles coincides and falls within the Service's mandate under the *CSIS Act*. But as a result of SIRC's review, the Committee concluded that there is an area where the two circles do not coincide.

SIRC recognizes that the Service has the statutory authority to collect information and intelligence for the TEL process, pursuant to Ministerial Direction to the Service. However, Ministerial Direction to CSIS cannot expand CSIS's mandate. It can only provide authority to CSIS to act within the limitations already established by the *CSIS Act*.

Overall, in the Committee's review of the Service's role in the TEL process, SIRC found that the Service's collection of information for the listing process was undertaken in accordance with Ministerial Direction—once this direction was provided[3]—and according to relevant operational policies. Nevertheless, SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to "threats to the security of Canada."

SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to "threats to the security of Canada."

The Committee is concerned by this extension of CSIS's collection activity, and by the lack of clear authority pertaining to that activity. After all, Parliament intended that the Service's collection activity would be precisely defined owing to the extraordinary powers exercised by CSIS.

SIRC's Ability to Review CSIS's Role in the TEL Process

The Special Senate Committee that originally examined Bill C-36 (the *Anti-Terrorism Act*) expressed concerns that the TEL process lacked adequate provisions for independent review. Senators were especially concerned at CSIS's involvement in the two-year review of the list, noting that, in effect, the list would be reviewed by the same people who created it.[4] As a result, Senators recommended that an Officer of Parliament position be created to review the TEL process or, alternatively, that SIRC be responsible for its two-year review.[5]

At that time, the Minister of Public Safety and Emergency Preparedness (who was then the Minister of Justice and Attorney General of Canada) argued that existing

3. SIRC notes that for the first year of the TEL process, CSIS performed its new duties without formal Ministerial Direction. The *National Requirements for Security Intelligence* 2003–2004 took effect April 1, 2003, fifteen months after passage of the *Anti-Terrorism Act*.
4. The Minister of Public Safety and Emergency Preparedness completed her first statutory review of the entity list on November 16, 2004.
5. Special Senate Committee on the Subject Matter of Bill C-36 "First Report" (November 1, 2001), page 5.

review mechanisms were sufficient. She stated: "We have ongoing oversight mechanisms that have proved effective, be that SIRC, be that the courts. Therefore, I would be disinclined to think about the creation of a new oversight mechanism that is separate and apart from those that exist."[6]

In February 2005, Senators raised this concern again with the Minister (as Minister of Public Safety and Emergency Preparedness) during her address to the Special Senate Committee on the *Anti-Terrorism Act*. Again, she cited SIRC as one of the "important safeguards and accountability mechanisms" with respect to the *Anti-Terrorism Act*.[7]

Given that the Minister specifically cited SIRC's ability to review the list as an important safeguard, the Committee believes it is important to note that although it can perform a fairly comprehensive review of the Service's role in the TEL process, SIRC cannot perform a complete review because it cannot see the Security Intelligence Reports upon which the Governor-in-Council's decisions are based, owing to Cabinet confidence. SIRC accepts that Section 39(3) of the *CSIS Act* prevents the Committee from gaining access to a Cabinet confidence. In the past, however, on the few occasions when SIRC has encountered an issue of Cabinet confidence, SIRC reached agreement with past Solicitors General to satisfy its concerns.

Although it can perform a fairly comprehensive review of the Service's role in the TEL process, SIRC cannot perform a complete review because it cannot see the Security Intelligence Reports upon which the Governor-in-Council's decisions are based, owing to Cabinet confidence.

An additional, but lesser, concern in SIRC's review of the TEL process is that another agency, such as the RCMP, could prepare a Security Intelligence Report. The section of the *Criminal Code* on judicial review of the listing process refers to "any security or criminal intelligence reports considered in listing the applicant" (83.05 [6]a), but does not specify which Canadian department or agency might prepare those reports. The inclusion of the word "criminal" suggests the RCMP could play a role in this process.

In the event that the RCMP were to prepare a Security Intelligence Report for consideration by the Governor-in-Council in the TEL process, SIRC would have no jurisdiction to review the matter, since its mandate is restricted to CSIS's activity.

6. Hon. Anne McLellan, appearance before the Special Senate Committee on the Subject Matter of Bill C-36 (October 29, 2001). She also said: "There are oversight bodies now. You have mentioned SIRC. SIRC will take up any enhanced obligations as a body of oversight as it relates to CSIS in their more concerted effort to root out and prevent terrorist activities."
7. Hon. Anne McLellan, appearance before the Special Senate Committee on the *Anti-Terrorism Act* (February 14, 2005).

SIRC's Actions

On the issue of Cabinet confidence, SIRC has raised the issue directly with the Minister when the Committee Members met with her in February 2005. The Committee also summarized its concerns in two letters to the Minister in December 2004 and

Collecting, Analyzing and Retaining Information on Threats to the Security of Canada

CSIS derives its primary authority to collect, analyze and retain information and intelligence from Sections 2 and 12 of the *CSIS Act*. It is an essential feature of almost every review conducted by SIRC to determine whether the Service carried out its duties and functions in accordance with these two sections of the *Act*.

Section 12 of the *Act* states:

> *"The Service shall collect, by investigation or otherwise to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report and advise the Government of Canada."*

Section 2 of the *Act* defines threats to the security of Canada as:

a) *espionage or sabotage that is against Canada or is detrimental to the interests of Canada, or activities directed toward or in support of such espionage or sabotage;*

b) *foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;*

c) *activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and*

d) *activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.*

Lawful advocacy, protest or dissent, are specifically excluded, unless carried out in conjunction with the enumerated threats.

March 2005. This concern was reinforced by SIRC's April 18, 2005, appearance before the Special Senate Committee on the *Anti-Terrorism Act*, and on June 8, 2005, before the House Sub-Committee. **The Committee is disappointed to note that, at the time of publication of this report, SIRC had still not received a response.**

On the issue of Cabinet confidence, SIRC has raised the issue directly with the Minister when the Committee Members met with her in February 2005.

As the Senate Committee noted in their original report on Bill C-36, "the erroneous placement of a person or group on this published list could cause irreparable harm."[8] The Committee recognizes the significant civil libertarian issues involved in the TEL process and takes seriously the concerns raised in this review.

Review of CSIS's Investigation of Transnational Criminal Activity

Report # 2004-02

Background

This review assessed CSIS's investigation of transnational criminal activities (TCA) and focussed on the Canadian-based activities of several foreign-based, transnational organized crime groups. This is the second SIRC study on this subject, following Report #107, issued in 1998 (SIRC 1998-01).

In 1995, member states of the G7 (including Canada) agreed to recognize international criminal activity as a national security threat. Since 1996, the Solicitor General of Canada (now the Minister of Public Safety and Emergency Preparedness) has directed CSIS to investigate TCA as part of its annual National Requirements for Security Intelligence. Accordingly, it has been identified as a subject of concern in the Service's annual counter-intelligence (CI) planning since 1995–1996. Investigations are conducted by the Counter Intelligence Branch's TCA Units, which are located in regions across Canada.

The investigations sampled for this review were national in scope and subject to Level II and Level III targeting investigations into suspected threat-related activities as described in Section 2(b) of the *CSIS Act*. This section of the *Act* defines the Service's intelligence role in relation to TCA. The previous study by SIRC emphasized the need for the

8. The Special Senate Committee on the Subject Matter of Bill C-36 "First Report" (November 1, 2001), page 5.

Service to differentiate carefully its national security role from criminal investigations conducted by law enforcement bodies/agencies.[9] In this review, SIRC was mindful of that finding.

Methodology

The review was undertaken pursuant to SIRC's mandate under Sections 38(b) and 40 of the *CSIS Act*. SIRC selected an eight-month review period from September 1, 2002, to April 30, 2003, and reviewed a list of the Service's TCA targets to select an issue-based targeting authority and four individual targets. This offered an opportunity to review various targeting processes outlined in operational policy, including the introduction of a new investigation, a renewal and an upgraded (Level II to III) investigation.

The review sought answers to the following questions:

- Did the Service have reasonable grounds to suspect a threat to the security of Canada?
- Was the level and intrusiveness of the investigation proportionate to the seriousness and imminence of the threat?
- Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?
- Was information exchanged with domestic and foreign agencies carried out in accordance with Sections 13 and 17 of the *CSIS Act*, as well as operational policies?

Overall, the operations reviewed were conducted in accordance with the *CSIS Act*, Ministerial Direction and operational policy and the techniques employed by the Service were consistent with the approved targeting levels.

To respond to these questions, SIRC examined all hard-copy and electronic documentation reported in the review period, and assessed these for compliance with the *CSIS Act*, Ministerial Direction, National Requirements and operational policy. Specifically, SIRC reviewed:

- targeting decisions and investigations of a sample selection of targets;
- the Request for Targeting Authorities (RTAs) and supporting operational reports; and
- cooperation and exchanges of information with domestic and foreign partners.

9. SIRC *Annual Report* 1998–1999, page 7.

Findings

SIRC concluded that CSIS had reason to believe that the activities of the four individual targets were foreign-directed or undertaken on behalf of foreign interests, and generally represented a threat as defined in Section 2(b) of the *CSIS Act*. In addition, SIRC found that the Service complied fully with Ministerial Direction and operational policy in applying for targeting authorization. It also applied a level of intrusiveness proportionate to the suspected threats.

Overall, the operations reviewed were conducted in accordance with the *CSIS Act*, Ministerial Direction and operational policy and the techniques employed by the Service were consistent with the approved targeting levels.

Section 12 of the *CSIS Act* authorizes the collection of information on suspected threats to the security of Canada. The Service then advises the Government of Canada about activities that may be suspected of constituting threats to the security of Canada.

> The Committee found that the Service's investigative practices in the area of transnational criminal activities have improved considerably and that there were comparatively few cases where tactical information was collected or retained.

SIRC found that the vast majority of information collected by CSIS on TCA within the review period was, indeed, strictly necessary to fulfill its mandate.

However, SIRC did note one instance in which information collected under Section 15 was inappropriately transferred to a Section 12 investigation. Section 15 of the *CSIS Act* allows the Service to conduct investigations for the purpose of providing security assessments. SIRC was concerned that the transfer of information originally collected as part of a Section 15 interview did not always meet the threshold of "strictly necessary." In this instance, SIRC believes the Service unnecessarily transferred personal, professional and employment information from a Section 15 interview to the operational reporting for the TCA Section 12 investigation.

Since the subject of the interview was not a target, SIRC concluded that this reporting exceeded reasonable requirements for background data and context. SIRC intends to monitor the operational reporting of information collected in Section 15 interviews to ensure that the Service operates in compliance with the *CSIS Act* and operational policy.

In its 1998 review, the Committee concluded "that the investigative threshold meant to distinguish strategic from tactical intelligence was [not] adequately defined" and,

as a result, CSIS collected and retained information on "tactical, street-level criminal activities that were clearly not within the scope of the Service's strategic objectives."[10]

In this study, the Committee found that the Service's investigative practices in the area of transnational criminal activities have improved considerably and that there were comparatively few cases where tactical information was collected or retained.

Information relevant to criminal investigations was provided to law enforcement agencies consistent with Section 17 of the *CSIS Act*. Similarly, foreign exchanges were within the scope of established arrangements with those agencies. SIRC found that exchanges of information between the Service and domestic and foreign partners were

Targeting

CSIS establishes a targeting level to investigate the activities of persons or organizations when it has reasonable grounds to suspect that these activities are a threat to the security of Canada. The conditions for approval of a targeting level are set out in detail in CSIS operational policy. Authority to administer, review and approve requests for targeting levels rests with the Target Approval and Review Committee. This committee is chaired by the Director of CSIS and includes several senior Service staff, General Counsel (Department of Justice), and a representative of the Deputy Minister of Public Safety and Emergency Preparedness Canada.

There are three levels of investigation:

Level I

- Allows for the use of minimally intrusive investigation techniques. Investigations are for short durations and allow CSIS to collect information from open sources and from records held by domestic and foreign police, security or intelligence organizations.

Level II

- Allows for the use of moderately intrusive investigation techniques. Investigations may include personal interviews and limited physical surveillance.

Level III

- Allows for the use of the most intrusive investigation techniques available, as outlined in Section 21 of the *CSIS Act*. The use of these techniques is subject to the most stringent judicial controls.

10. SIRC *Annual Report* 1998–1999, page 7.

accompanied by appropriate caveats. Moreover, they complied with operational policy as well as relevant Memoranda of Understanding.

While reviewing the issue-based investigation, the Committee noted a series of events that demonstrated particularly effective use of domestic and foreign arrangements. In this case, the Service assessed that certain information provided to it by another domestic agency was a threat to the life of an individual. Although not obligated to do so, the Service quickly obtained permission from the domestic agency to disclose pertinent information and forwarded it to a foreign partner agency. These actions may have thwarted an attempt on the individual's life.

There were no recommendations arising from this review.

Review of a Counter-Terrorism Investigation

Report # 2004-05

Background

For this study, SIRC examined a CSIS counter-terrorism investigation that had not been the focus of a comprehensive SIRC review in over a decade, yet has remained a high priority of the Counter Terrorism Branch. This investigation was the subject of a Level III targeting authority for suspected threat-related activities as described in Section 2(c) of the *CSIS Act*.

Methodology

At the outset, SIRC examined lists of all CSIS targets, warrants and human sources related to the Service's investigation. The Committee then selected for in-depth review one issue-based target, one targeted organization, six individual targets, one warrant and six human source operations. For each file, all electronic and hard-copy documentation was reviewed for the period from January 1 to December 31, 2003. To ensure a thorough review, SIRC also examined some documentation that was outside the review period.

As in other reviews of CSIS investigations, SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining key operational activities:

- targeting decisions and investigations;
- acquisition and execution of warrant powers and special operations;
- management of human sources and sensitive operations;

- cooperation and exchanges of information with domestic partners;
- cooperation and exchanges of information with foreign partners; and
- advice to government.

SIRC sought to determine whether:

- CSIS had reasonable grounds to suspect a threat to the security of Canada;
- the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat; and
- the Service collected only information that was strictly necessary to fulfill its mandate to advise the Government of a threat.

Findings

SIRC found that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that the targets of the investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat.

SIRC did seek clarification as to why an individual remained a target of investigation for several months following his departure from Canada. The Service's explanation satisfied SIRC that the delay in terminating the investigation against this target was reasonable.

SIRC did seek clarification as to why an individual remained a target of investigation for several months following his departure from Canada.

Overall, the Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy. CSIS collected only the information that was strictly necessary to fulfill its mandate.

The Service met all of the requirements of the *CSIS Act* and operational policy with respect to warrant acquisition. SIRC found that CSIS had information to support all of the factual statements in the affidavit. Moreover, the affidavit was complete and balanced—the facts and circumstances of the case were fully, fairly and objectively expressed.

SIRC found that the Service, in implementing the powers authorized by the warrant, complied with the *CSIS Act*, operational policy and the conditions imposed by the Federal Court. However, SIRC found that existing operational policy did not provide sufficient guidance concerning certain administrative procedures related to the execution of some warrant powers. The Service advised that new operational policy

to address this shortcoming had been approved. SIRC also followed up on an issue of non-compliance with operational policy by a CSIS regional office that was noted in SIRC Study 2003-04, and found no problems of this nature in this investigation.

The human source operations were well managed by the Service and complied fully with Ministerial Direction and operational policy. The administrative and financial files for each operation were in good order. Moreover, SIRC found that CSIS appropriately managed the relationships with sources used in sensitive areas.

SIRC found that existing operational policy did not provide sufficient guidance concerning certain administrative procedures related to the execution of some warrant powers.

SIRC also assessed, against the backdrop of evolving legislation, the adequacy of the Service's human source operations policies, and found that current policies were sufficient. The Committee will continue to monitor this operational activity closely in future reviews.

The Committee found no problems or issues of concern with respect to the Service's dealings with domestic and foreign partners. Exchanges of information with these agencies complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC brought to the Service's attention a small number of administrative errors or omissions in operational reporting, which the Service has subsequently corrected.

Finally, SIRC pursued an issue raised in SIRC Study 2003-02 concerning the implications of the *Anti-Terrorism Act*. This study raised concerns regarding the payment of human sources. SIRC asked the Service if it had reviewed its policies or guidelines concerning source compensation. In reply, the Service informed the Committee that it had received legal advice which indicated that its approach was appropriate.

In future reviews, SIRC intends to monitor the Service's human source operations involving listed terrorist entities, to identify any issues of concern and to re-evaluate the adequacy of operational policy in this area. There were no recommendations arising from this study.

Issue-Based Targeting

This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects that there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not yet been identified. As in any other targeting procedure, if warrant powers are requested, approval must be granted by the Federal Court of Canada. Operational policy dictates that as soon as individual persons, groups or organizations are identified as taking part in threat-related activities in connection with an issue or event, the Service will seek separate targeting authority.

It continues to be the Committee's practice to assess all issue-based investigations on a case-by-case basis to ensure they are conducted appropriately.

Review of Activities and Investigations in a CSIS Regional Office

Report # 2004-04

Background

SIRC endeavours each year to undertake a comprehensive review of CSIS's activities in a particular region of Canada. This type of review looks across the board at the targeting of individuals, implementation of warrant powers, use of human sources, as well as cooperation and exchanges of information with Canadian and foreign partners. It provides unique insights into the ways CSIS employs various investigative tools at its disposal — in addition to the standard assessment of CSIS's compliance with the *CSIS Act*, Ministerial Direction and operational policies.

Methodology

SIRC selected a regional office, examining its activities for the period April 1, 2002–March 31, 2003. As a first step, the Committee examined preliminary data on all active investigations in 2002–2003. Based on this examination, it decided to focus its review on a specific counter-terrorism investigation, which became a counter-proliferation investigation in July 2002.

SIRC reviewed all hard-copy and electronic documentation during the review period, pertaining to five types of CSIS operational activities:

- the targeting of individuals suspected of engaging in threat-related activities, as well as the targeting approval process;

- the implementation of warrant powers against authorized targets;
- special operations enabling the execution of warrant powers;
- the direction of human sources against authorized targets; and
- exchanges of information with other domestic and foreign law enforcement and security intelligence agencies.

SIRC also reviewed CSIS's internal security measures for the region, as well as any security violations and breaches between April 1, 2000 and March 31, 2003.

As in all reviews, SIRC sought to answer three key questions:

- whether CSIS had reasonable grounds to suspect a threat to the security of Canada;
- whether the level of targeting authority was proportionate to the threat; and
- whether the Service only collected information strictly necessary for its investigation.

SIRC conducted an on-site visit to gain a better understanding of the nature of regional operations and of the unique challenges that Service investigators face in the region under review.

Findings

Overall, the region's investigative activities during the review period complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada, and that the intrusiveness of the techniques used were proportionate to the suspected threat these targets posed.

Warrant powers, such as telephone intercepts, are the most intrusive investigative techniques available to CSIS. These powers are granted by the Federal Court of Canada. SIRC found that CSIS complied with the terms of the Federal Court warrant in executing warrant powers, as well as conducting special operations during the review period. CSIS only used warrant powers that were necessary to further its investigation. It did not renew them where the other powers available through the targeting authority were sufficient. The Service also acted appropriately and within the law in directing human sources, as well as in exchanging information with other agencies.

Section 12 of the *CSIS Act* restricts CSIS to collecting information that is "strictly necessary" for its investigations of threat-related activities. SIRC found that, in general, CSIS had collected only that information that was strictly necessary to its investigation. In one instance, however, the Committee believes CSIS collected and reported personal information that approached the limit of what is allowed under the *Act*.

During the review, SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. CSIS assessed that certain activities taking place were not a significant aspect of the organization, believing that it served primarily one purpose.

SIRC carefully examined all documentation referring to the organization. It also looked at information on file from a previous review of the same investigation. Based on this, the Committee found that the organization had a dual function.

SIRC believes operational policy governing certain types of investigations should apply to this organization. CSIS disagreed with this finding.

The Committee recognizes that in such situations, it can be difficult to determine which operational policy is applicable. Accordingly, SIRC recommended that CSIS define one particular term in its operational policy.

The Committee also found one instance in which CSIS did not fully comply with operational policy. CSIS did not agree with this finding. Apart from these issues, SIRC noted a few administrative errors in CSIS's implementation of warrant powers, use of human sources, and exchanges of information. These errors were minor and did not affect CSIS's investigations. Further, the Committee was informed that CSIS has made changes to prevent their reoccurrence.

SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. CSIS assessed that certain activities taking place were not a significant aspect of the organization, believing that it served primarily one purpose ... SIRC believes operational policy governing certain types of investigations should apply to this organization. CSIS disagreed with this finding.

Also of note, SIRC reviewed security practices and procedures that had been in use in the region under review since 2000. There was one breach of security, which gave rise to a related complaint that was investigated by SIRC under Section 42 of the *CSIS Act*.[11]

11. Security violations are less serious than security breaches. Violations are defined as any contravention of security policies, such as the failure to lock up classified information. Breaches occur when any classified information or asset is the subject of unauthorized access or disclosure.

Review of a Counter-Proliferation Investigation

Report # 2004-09

Background

In July 2002, the Canadian Security Intelligence Service created the Counter Proliferation (CP) Branch, bringing together elements of investigations that were previously the responsibility of the Counter Terrorism (CT) and Counter Intelligence (CI) Branches. In 2004, SIRC undertook a review of this branch—its first opportunity to examine the Service's counter-proliferation activities under the new organizational structure.

Methodology

This study examined the Service's investigation, between January 1, 1999, and December 31, 2003, of the threat to Canadian security posed by activities related to the proliferation of weapons of mass destruction by persons or organizations linked to a certain country. To ensure a thorough review, SIRC also examined some material outside the scope of the review period.

The Committee reviewed the Service's issue-based investigation. In addition, SIRC staff met with officials from the Service's CP Branch to discuss certain aspects of this investigation.

As with all reviews of this nature, SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining the following key operational activities:

- targeting decisions;
- investigative activities and operational reporting;
- cooperation and exchanges of information with domestic partners;
- cooperation and exchanges of information with foreign partners; and
- advice to the federal government.

SIRC sought to determine whether:

- CSIS had reasonable grounds to suspect a threat to the security of Canada;
- the level and intrusiveness of CSIS's investigation was proportionate to the seriousness and imminence of the threat; and
- the Service collected only information strictly necessary to fulfill its mandate to advise the federal government of a threat.

Findings

SIRC found that the Service complied fully with Ministerial Direction and operational policy with respect to the applications for targeting authorization. The statements made in the applications were supported by the Service's operational reporting. Based on the information in the Service's possession, SIRC concluded that the Service had reasonable grounds to suspect that each of the authorized targets of investigation posed a threat to the security of Canada.

The level and intrusiveness of the Service's investigation was proportionate to the suspected threat. CSIS collected only information strictly necessary to fulfill its mandate to advise the federal government of a threat.

SIRC endorsed the Service's approach of engaging relevant private-sector entities, undertaken via the Liaison Awareness Program (LAP). Providing CP briefings to the private sector not only assists the Service in meeting its operational requirements, but also provides a potentially valuable service to recipients who might be vulnerable to targeting by foreign entities. The LAP has provided leads in a number of cases and has fostered a cooperative spirit among industry representatives.

Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy.

Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy. SIRC found no problems or issues of concern with respect to the Service's cooperation with its domestic or foreign partners.

There were no recommendations arising from this review.

Review of CSIS's Information Operations Centre

Report # 2004-07

Background

In today's information age, hostile actors (e.g., extremists, terrorist groups, foreign intelligence services or armed forces) no longer need direct access to a computer to copy, destroy or manipulate data. Rather, a variety of techniques and software tools can be used to gain unauthorized remote access to exploit a targeted system. This type

of activity is called an "information operation," and in some cases it can pose a threat to national security. Canada's critical infrastructure[12]—which is dependent on computer networks—must be vigilant regarding such attacks. CSIS investigates the activities of those who are suspected of using information operations to threaten the security of Canada as defined under Section 2 of the *CSIS Act*.

Two thresholds must be met before CSIS begins investigating a suspected information operation:

(1) there must be reasonable grounds to suspect that the activity is sponsored by a foreign state (or one of its agents), a terrorist group, or politically motivated extremists; and
(2) the purpose of the attack must relate to espionage, sabotage, terrorism, foreign influenced activity or violence to achieve political, ideological or religious objectives.

In February 2002, to counter the threat posed by cyber-based attacks, CSIS established an Information Operations Centre (IOC), which is responsible for developing and using specialized investigative techniques.

Methodology

In 2004, SIRC undertook its first-ever review of CSIS's investigation of threats against Canada's critical information infrastructure. It did so with two objectives. First, SIRC reviewed the role of the IOC in investigating threats against Canada's critical information infrastructure. Second, the Committee reviewed the IOC's operations, examining one counter-intelligence investigation of an information operation for compliance with the *CSIS Act*, Ministerial Direction and Service operational policies.

In 2004, SIRC undertook its first-ever review of CSIS's investigation of threats against Canada's critical information infrastructure.

The review covered the period between January 1, 2000 and December 31, 2003.

Findings

Notwithstanding two concerns identified below, SIRC found that in carrying out its duties and functions, the Service complied with the *CSIS Act*, Ministerial Direction and CSIS operational policies.

12. The Government of Canada has identified 10 critical infrastructure sectors: energy and utilities; communications and information technology; finance; health care; food; water; transportation; safety; government; and manufacturing (Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, November 2004).

SIRC's first concern was that operational policy keep pace with the matter reviewed. The Committee recommended that the Service review its operational policies regarding Section 12 targeting in this area.

> **SIRC recommends that the Service review operational policy to ensure that it clearly incorporates certain matters in relation to Section 12 targeting.**

The Committee's second concern was related to administrative errors. SIRC found four such errors. While three of these were minor, the fourth involved the Service's operational reporting—which could potentially affect the role of the targeting approval process as a mechanism for internal accountability. SIRC recommended that the Service review operational reporting policies to prevent a reoccurrence of this error.

> **SIRC recommends that the Service review operational policy to ensure that if it is necessary to cross-reference operational database reports recorded under one file number with reports recorded under another file number, this should be noted in the "Investigator's Comments" section of the reports.**

The Service has indicated that it will be examining ways to ensure the cross referencing operational database messages when they are transferred from one investigative file to another.

Review of CSIS's Exchanges of Information with Close Allies

Report # 2004-08

Background

In January 2004, the federal government created the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor Commission). Former CSIS Director, Ward Elcock, defended CSIS's information-sharing practices, noting that SIRC had not made any criticism of the appropriateness or inappropriateness of any information CSIS had shared with any foreign agency in any cases it had reviewed since September 11, 2001.[13]

The case of Mr. Arar did, however, focus public attention on the use of information that may have been collected in Canada and then shared with Canada's foreign partners.

13. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. Transcript (June 22, 2004), page 277, line 21–23.

While SIRC has examined CSIS's information-sharing practices in the context of several past reviews, the Committee decided to undertake its first in-depth examination of CSIS's exchanges of information with close allied partners.

Methodology

Drawing on one of the Service's counter-terrorism investigations, SIRC chose to review CSIS's information exchanges with four allied agencies as the focus of the detailed review. This review covered the period June 1, 2003–December 31, 2003, but for thoroughness it also examined certain documentation that fell outside the review period. SIRC examined all relevant electronic and hard-copy documentation related to the investigation to determine if these exchanges about threats to the security of Canada were in accordance with the respective foreign arrangements for the four allied agencies and complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC looked at:

- the scope of the foreign arrangement;
- the consent or approval required to disclose such information;
- any special conditions or limitations placed on the use of this information; and
- the nature of the information being shared.

Findings

In the context of the investigation that was reviewed, SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy. The Committee also found that the Service exercised due diligence in exchanging information about targets of investigation.

SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy.

While the Service obtained appropriate approval prior to disclosing information to selected allied agencies, SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies. However, it was CSIS's position that ultimate accountability is clearly defined in policy.

SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies.

In this study, SIRC also examined how human rights were addressed within the context of foreign arrangements.

When CSIS initiates the process to enter into a new arrangement with a foreign agency, it informs Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness that it will "closely scrutinize the content of the information provided to, or received from, a foreign agency in order *to ensure* [our emphasis] that none of the information sent to, or received from, that agency is used in the commission of, or was obtained as a result of, acts that could be regarded as human rights violations."

SIRC took note of two issues arising from this statement.

First, the use of the term "ensure" implies that CSIS will make certain that the information shared does not lead to—or result from—acts that could be regarded as human rights violations. **However, the Committee concluded that CSIS was not in a position to provide such an absolute assurance.** As Mr. Elcock told the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, CSIS would not necessarily reject information that might have been obtained as a result of human rights violations. He explained that CSIS "[is] there to collect information... that may reflect on a threat to the security of Canada and we will look at information from any source in order to secure some information about threats to the security of Canada."[14]

Second, while CSIS is cautious when sharing information with foreign agencies, it cannot determine in all cases how that information is used by the recipient agency. Similarly, the Service is rarely in a position to determine how information received from a foreign agency was obtained. As Mr. Elcock stated to the O'Connor Commission, when it comes to information that may have been the product of torture, "the reality is in most cases we would have no knowledge that it was derived from torture. You may suspect that it was derived from torture, but that is about as far as one will get in most circumstances."[15]

> The Committee found that CSIS's assurance to the Minister could be misinterpreted as it is rarely in a position to determine how information that went to a foreign agency is used, or how information it receives was obtained.

14. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Transcript (June 21, 2004), page 162, line 15–19.
15. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Transcript (June 21, 2004) page 159, line 23–25; page 160, line 1–2.

In response to this study, the Service took the position that all correspondence between CSIS and the Minister of Public Safety and Emergency Preparedness reflects an ongoing monitoring of the situation. According to the Service, they advise the Minister that exchanges of information with an allied agency will be commensurate with the degree of trust established over a period of time and reflective of the political and human rights climate within a country.

SIRC acknowledges that CSIS must rely on information received from its foreign partners to fulfill its mandate, and that the exchange of information between security intelligence agencies is an essential investigative tool. However, the Committee found that CSIS's assurance to the Minister could be misinterpreted as it is rarely in a position to determine how information that went to a foreign agency is used, or how information it receives was obtained.

SIRC recommended that CSIS revise the content of the letters to Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness to avoid leaving any impression that it can guarantee that information sent to, or received from, a foreign agency was not used in the commission, nor was obtained as a result of, acts that could be regarded as human rights violations.

Review of a Counter-Intelligence Investigation

Report # 2004-06

Background

In this review, SIRC examined a CSIS investigation of a foreign intelligence service.

Methodology

SIRC examined this counter-intelligence investigation for the period January 1, 2003 to December 31, 2003. The objective was to assess the Service's compliance with the *CSIS Act*, Ministerial Direction and all relevant operational policies.

SIRC reviewed hard-copy and electronic documentation that pertained to the following CSIS operational activities:

- targeting of individuals suspected of engaging in threat-related activities, as well as the targeting approval process;
- application for a Federal Court warrant;
- implementation of warrant powers against authorized targets;
- direction of human sources against authorized targets; and
- selected advice to government departments.

As in all reviews, SIRC sought to answer three key questions:

- whether CSIS had reasonable grounds to suspect a threat to the security of Canada;
- whether the level of targeting authority was proportionate to the threat; and
- whether the Service only collected information that was strictly necessary for its investigation.

Findings

Overall, the counter-intelligence investigation was in compliance with the *CSIS Act*, Ministerial Direction and operational policy during the review period. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada. Moreover, the Committee found that the intrusiveness of the techniques used were proportionate to the suspected threat that these targets posed. CSIS investigators only collected information that was strictly necessary for the investigation. They also acted appropriately and within the law in their use of human sources.

SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada.

SIRC found that the Service's description of threat-related activities in the warrant affidavit accurately reflected the information that CSIS held. The Service complied with all applicable operational policies in applying for the warrant, as well as conditions imposed by the Federal Court when the warrant was approved. SIRC also found that CSIS complied with the terms of the Federal Court warrant in executing authorized warrant powers and in conducting special operations.

The Committee observed, however, that the scope of the warrant was overly ambitious. Two CSIS regions identified human resource shortages that affected their ability to analyze certain information collected. SIRC also noted that CSIS introduced a new information collection technique during the review period, which will be monitored in future reviews.

SIRC paid particular attention to CSIS's investigation of interference activities.

Throughout the review, SIRC paid particular attention to CSIS's investigation of interference activities. To ensure compliance with the *CSIS Act*, the Service was careful to develop strict guidelines to manage this aspect of its investigation. However, SIRC

found that CSIS's operational policies covering these types of situations were incomplete. Because of this, the Committee recommended that:

> **CSIS review and amend, where appropriate, its operational policies relating to specific institutions to ensure that they cover all aspects of a given process.**

Also of note, while SIRC found that CSIS acted appropriately in providing advice to Government of Canada officials on the foreign intelligence service's activities, the Committee nevertheless believes that the Service was overly cautious in deciding not to share information with one federal department. CSIS disagreed with this finding and believes that given the sensitivity of the investigation, the Service took a judicious approach in the dissemination of any information.

Terrorist Financing Activities in Canada

Report # 2004-10

Background

Since September 11, 2001, the international community has increased its efforts to combat terrorist financing. In December 2001, the United Nations Security Council passed Resolution 1373, calling on member states to freeze the assets of those who commit or facilitate terrorist acts, and to adopt measures to prevent and suppress the financing of terrorism. In response, the Government of Canada passed the *United Nations Suppression of Terrorism Regulations* (UNSTR) and the *Anti-Terrorism Act*.

Traditionally, CSIS had examined terrorist financing through the lens of its counter-terrorism investigations, but the growing international focus since September 11, 2001, necessitated the development of a dedicated level of expertise. In 2002, CSIS created the Terrorist Financing Unit within its Counter Terrorism Branch to identify and track the financial structures that support terrorist organizations. That same year, the Minister's *National Requirements for Security Intelligence* specifically directed CSIS, for the first time, to investigate and advise the Government of Canada about the threat arising from terrorist financing.

Methodology

The objective of this study was to examine CSIS's investigation of terrorist financing activities in Canada for in-depth review. SIRC selected one issue-based target, and five specific targets. In each case, the Committee assessed the Service's compliance with

the *CSIS Act*, Ministerial Direction and operational policy by examining the following operational activities:

- targeting decisions;
- investigative activities and operational reporting;
- cooperation and exchanges of information with domestic agencies; and
- cooperation and exchanges of information with foreign agencies.

SIRC's review period was January 1, 2003–July 31, 2004. However, to ensure a thorough review, the Committee also examined select documents that fell outside this period.

Findings

The Committee concluded that the Service had reasonable grounds to suspect that the activities of targeted individuals and groups posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat, and CSIS collected only that information necessary to fulfill its mandate. The Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC also found that the Service complied fully with Ministerial Direction and operational policy with respect to applications for targeting authorizations and renewals. The statements made in the applications were supported by the Service's operational reporting.

Finally, SIRC was satisfied with the degree and nature of the Service's cooperation with domestic and foreign partners. Exchanges of information with these agencies complied with the *CSIS Act*, Ministerial Direction, and operational policy.

Implementation of the UNSTR

During this review, SIRC learned that the implementation of the UNSTR required CSIS to manage new responsibilities related to the listing of terrorist entities. The Committee did not undertake a comprehensive review of CSIS's involvement in the listing of entities pursuant to the UNSTR, as this was not within the scope of the study. However, SIRC noted that CSIS's involvement in this process raised important legal questions—similar to those identified in the Committee's review of the Terrorist Entity Listing Process.

The criteria for listing under the UNSTR are set out in Section 2 of the legislation, which states that a person or group can be listed when there are reasonable grounds to believe that this entity: (a) has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity; (b) is controlled directly or indirectly by any person conducting any of the activities set out in paragraph (a); or (c) are acting

on behalf of, or at the direction of, or in association with any person conducting any of the activities set out in paragraph (a).

Entities can be listed in two ways. First, they can be placed under a UN Security Council resolution, in which case they are then automatically included as a listed entity under the *United Nations Afghanistan Regulations* (UNAR). Second, the Governor-in-Council, on the recommendation of the Minister of Foreign Affairs, can decide to place an entity on the UNSTR list. In such cases, Foreign Affairs Canada (FAC) convenes an interdepartmental meeting to discuss the proposed listing. If CSIS has security intelligence on the entity, it prepares an assessment for its Director, indicating whether there are reasonable grounds to support the listing. This assessment is provided to FAC, who may use the information, along with input from many other federal departments and agencies, to support its recommendation to the Governor-in-Council.

The Service told SIRC that it engages in the listing of entities pursuant to the UNSTR under Section 12 of the *CSIS Act*, which limits the Service's collection activity to *threats to the security of Canada*. However, SIRC noted that the Service's involvement in the listing process requires it to determine whether an entity meets the definition of a *listed person* under the UNSTR, which has no such geographic restriction. As a result—similar to SIRC's study on the Terrorist Entity Listing Process—it is possible that the Service may be required to collect and analyze information regarding an entity that meets the definition of a *listed person or group* under the UNSTR, but does not represent a *threat to the security of Canada*. SIRC found evidence of this problem in its review of operational reports.

In response to SIRC's concern relating to the UNSTR listing process, CSIS stated that they are only collecting and analyzing open information. The Service does not agree that the collection and retention of open information that is available to the public is an extension of the Service's mandate.

In response to SIRC's concern relating to the UNSTR listing process, CSIS stated that they are only collecting and analyzing open information. The Service does not agree that the collection and retention of open information that is available to the public is an extension of the Service's mandate. Further, SIRC noted that the UNSTR does not specifically direct the Service to participate in the listing process, nor has the Minister of Public Safety and Emergency Preparedness provided CSIS with specific direction to that effect. Indeed, the *National Requirements for Security Intelligence 2003–2004* only made reference to the *Criminal Code* listing process, requiring that CSIS continue to conduct research and analysis in support of the listing of terrorist entities pursuant to the *Anti-Terrorism Act*.

SIRC will continue to monitor this issue. As always, it will continue to examine the implications of new legislation on the Service's operational activities. There were no recommendations arising from this study.

CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post

Report # 2004-01

Background

Security liaison posts are located strategically to meet the needs of the Service most effectively. CSIS's Foreign Liaison and Visits (FLV) Branch, which oversees the security liaison posts abroad, bases its operations on the principle of reciprocity. The Service must be prepared to share information with foreign security and intelligence agencies to receive information in return. Activities and exchanges of this nature are generally handled by the Service's security liaison posts. With the exception of Paris, Washington, and London, the locations of these posts are classified.

At the direction of the FLV branch, Security Liaison Officers (SLO):

- carry out regular liaison with foreign security and intelligence agencies;
- provide security screening services in support of the immigration program;
- oversee the exchange of security intelligence information with approved agencies;
- provide advice to senior staff of the Canadian Mission or Embassy; and
- are accountable to the Director General of FLV, to HQ operational managers, and to the Head of Mission for the SLO's geographical area of responsibility.

SIRC regularly reviews the Service's security liaison posts, as required under Section 38(a)(iii) of the *CSIS Act*. This year, SIRC chose to review a recently established security liaison post.

Methodology

In its review, SIRC sought to determine whether exchanges of information from this post with foreign agencies were within the scope of the government-approved liaison agreements in place. The Committee also assessed the operations at the security liaison post in relation to the *CSIS Act*, Ministerial Direction, and the Service's operational policies and procedures.

SIRC conducted this study by reviewing documents at CSIS Headquarters and through an on-site visit to the security liaison post. For context, SIRC also reviewed this

post's operations, and evaluated them against issues raised in SIRC's ongoing statutory reviews of CSIS's Foreign Arrangements. Moreover, the report considered trends identified in SIRC's SLO studies over the previous five years.

The review concentrated on two main issues: security screening workload and security at the post.

Findings

a) Compliance and Effectiveness

There were not enough exchanges during the review period for SIRC to assess definitively whether the Service's exchanges with foreign agencies at the Post were in accordance with the *CSIS Act*, Ministerial Direction and the Service's operational policies. However, SIRC's review of the exchanges that did take place suggests that the Service has approached its new liaison relationship with appropriate caution.

The lack of updated CSIS documents to assess the liaison relationships at the post did cause SIRC some concern.

However, the lack of updated CSIS documents to assess the liaison relationships at the post did cause SIRC some concern. While there are written guidelines for the creation, submission and updating of these documents, there are no formal CSIS policies governing this activity. Owing to the situation SIRC observed at this post, and the Service's growing exchanges with foreign organizations, the Committee made the following recommendation:

> **The Committee recommended that the Service create policies for the preparation, updating and annual submission of CSIS documents used to assess exchanges with foreign agencies.**

The Committee also recommended that the written guidelines the FLV prepares concerning procedures at security liaison posts be updated to reflect actual Service practices.

b) Security Screening

One of the functions of an SLO is to assist Citizenship and Immigration Canada and the Canadian Border Services Agency to screen potential immigrants to Canada. If the employees of either of these organizations responsible for immigration screening at a security liaison post have security-related concerns, they may refer the case to the SLO, who investigates the matter.

SIRC notes that the SLO's security screening workload has been raised as a concern in each of its SLO studies over the past five years. In its most recent report, SIRC again raised concerns related to security screening workload and suggested the Service adopt numeric benchmarks for tracking and addressing security screening workload issues.

c) Security at the Post

SIRC examined the environment in which the post operated. The Committee concluded that the SLOs at the post acted in accordance with CSIS security procedures.

The Role of CSIS Security Liaison Officers

CSIS Security Liaison Officers perform the following functions on behalf of the Service when based in foreign posts:

- they maintain and develop channels of communication with foreign agencies with which the Service has approved arrangements;
- they carry out security screening activities in support of the federal Immigration Screening Program;
- they report to CSIS Headquarters on any matter related to Canadian security interests; and
- they undertake specific reliability checks as requested by the Mission Security Officer.

Any operational assistance or investigative activity related to threats to the security of Canada (Section 2 of the *CSIS Act*) that CSIS may undertake outside Canada are separate and distinct from the Security Liaison Officer's functions and responsibilities.

Review of Foreign Arrangements

Background

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with the government of a foreign state, or an international organization of states (or an institution thereof), for the purpose of performing its duties and functions. While Ministerial Direction and Service operational policy outline the principles regarding the establishment and management of such arrangements, the foreign arrangement determines the nature and extent of the Service's cooperation and exchanges with a foreign agency. The arrangement identifies the specific types of information sharing that can occur.

Section 38(a)(iii) directs SIRC to review all such arrangements. The Committee examines both the establishment and enhancement of arrangements entered into between CSIS and foreign intelligence agencies.

As noted in previous reports, a Ministerial Direction Compendium came into effect on March 1, 2001. This gives the Director of CSIS more freedom to manage the Service's activities. For example, the Director can approve the expansion of an existing foreign arrangement (one that has previously been approved by both the Minister of Public Safety and Emergency Preparedness and the Minister of Foreign Affairs). CSIS does not need to consult with the Department of Foreign Affairs nor does it need to request the Minister's approval to do so. As a result, the Director has greater discretion in this area of Service activity.

Reviews During 2004–2005

During 2004–2005, SIRC undertook its first comprehensive review of the expansion process—a first since the Ministerial Direction Compendium came into effect. SIRC focussed on the ten arrangements that were expanded between April 1, 2002 and March 31, 2003, to determine whether these complied with Ministerial Direction and operational policy. An enhancement or expansion occurs when the Service changes an existing arrangement. This defines the subject matter and extent of authorized exchanges.

SIRC undertook its first comprehensive review of the expansion process—a first since the Ministerial Direction Compendium came into effect.

For each foreign arrangement, SIRC staff examined:

- the rationale for requesting an expansion;
- Canada's national security interests;
- the request to expand the arrangement;
- the approval to expand the arrangement; and
- the Service's assessment of the agency (i.e., respect of the third-party rule, reliability, human rights issues, internal stability concerns, etc.)

Staff reviewed:

- all documentation on the establishment of the arrangement, as per Section 17 of the *CSIS Act* and Ministerial Direction;
- all documentation on the expansion of the arrangement;
- the cooperation file with the organization;
- the most recent agency assessment;
- the most recent post profile prepared by the Security Liaison Officer; and
- any other information related to the arrangement and its enhancement.

Findings

SIRC found that CSIS complied with the conditions set out in Ministerial Direction and operational policy regarding the expansion of the ten existing foreign arrangements.

With respect to expansion approvals, SIRC noted that the Service has no operational policy on what type of information must be contained in the request submitted to the Director. The Committee also noted that the assessment of agencies with whom the Service has arrangements were not always submitted on a yearly basis as required in the Foreign Liaison Post Procedures Manual—and, in some cases, were seriously outdated. The matter of agency assessments was the subject of a recommendation under study # 2004-01.

One agency assessment did not provide an adequate analysis of potential human rights issues.

Of greater concern to SIRC, however, was that one agency assessment did not provide an adequate analysis of potential human rights issues. As these expansions involve an increased level of cooperation with a foreign agency, SIRC believes that a comprehensive re-evaluation of the agency in question should be required at the time of expansion to ensure that arrangements continue to undergo rigorous scrutiny—particularly in the area of human rights.

It is CSIS's position that when consideration is being given to expanding the arrangement, FLV provides the requisite information so that the Director can make an informed decision as to whether a given arrangement should be expanded. According to the Service, the absence of an up to date Agency Assessment does not mean that a review of the arrangement has not been prepared for the Director.

Policy Direction for Foreign Arrangements

The *CSIS Act* gives CSIS the authority to enter into arrangements with agencies of foreign governments and international organizations. Such arrangements must be approved by the Minister of Public Safety and Emergency Preparedness after consultation with the Minister of Foreign Affairs. Ministerial Direction dictates the procedures and conditions necessary to establish a new arrangement, or to expand an existing one. Moreover, it gives the Director of CSIS authority to manage existing arrangements, subject to any conditions imposed by the Minister.

Ministerial Direction requires that arrangements meet the following criteria:

- they must be established as required to protect Canada's security;
- they must remain compatible with Canada's foreign policy objectives toward the country or international organization in question;
- they must respect the applicable laws of Canada; and
- the human rights record of the country or agency is to be assessed, and the assessment weighed in any decision to enter into a cooperative relationship.

The nature of the relationship between CSIS and a foreign organization is established when CSIS enters into an arrangement that allows the Service to exchange information or cooperate in specific areas. CSIS may also expand arrangements to include specific exchanges of information or restrict them in certain areas.

B. Investigations of Complaints

In addition to its review function, SIRC is responsible for investigating complaints from the public about CSIS. Four kinds of complaints may be directed to the Committee for investigation:

- complaints lodged by persons "with respect to any act or thing done by the Service" (Section 41);
- complaints received concerning denials of security clearances to government employees or contractors (Section 42);
- referrals from the Canadian Human Rights Commission of complaints made to it; and
- Minister's reports in respect of the *Citizenship Act*.

Where appropriate, SIRC investigates complaints through a quasi-judicial hearing presided over by a Member of the Committee.

Through its investigation of complaints, SIRC determines whether the Service's activities have been carried out in accordance with the *CSIS Act*, Ministerial Direction and CSIS policy.

Following Section 41 investigations, SIRC is required, under the *CSIS Act*, to provide the Minister and the Director of CSIS with a report containing the findings of the investigation and any recommendations the Committee considers appropriate. The *Act* also directs SIRC to report to the complainant its findings and, if the Committee considers it appropriate, any recommendations made to the Minister and Director.

Following a Section 42 investigation, SIRC provides the Minister, the Director of CSIS, the deputy head of the government agency concerned and the complainant with a report containing any recommendations the Committee considers appropriate and those findings the Committee considers fit to report to the complainant.

Table 1 provides that status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside the Committee's jurisdiction or investigated and resolved without a hearing (administrative review).

Table 1
Resolution of Complaints*

Description	2002–2003	2003–2004	2004–2005
Carried over	17	17	16
New	48	30	30
Total	**65**	**47**	**46**
Closed	48	31	28
Carried forward to subsequent year	17	16	18

* The Table reflects all complaints received by SIRC. However, not all complaints received resulted in an investigation by the Committee. Some were redirected to the appropriate government institutions, or were determined at the outset to be outside the Committee's jurisdiction, while others were withdrawn by the complainants.

Reports of Decisions: Case Histories

The following are summaries of the three decisions rendered by SIRC during the period under review in response to complaints filed with the Committee.

REPORT: HUMAN RIGHTS COMPLAINT REFERRAL

SIRC reported a decision concerning a complaint that was referred to the Committee by the Canadian Human Rights Commission under Section 45 of the *Canadian Human Rights Act* (CHRA).

The complaint alleged discrimination in contravention of the CHRA by the Service. More particularly, the complainant—a former employee of the Service—complained that the Service had failed to adjust hours of work and to allow time away from work, and thereby failed in its duty to accommodate the complainant's physical and mental disabilities.

The Committee concluded that the Service did not fail in its duty to accommodate the complainant, and did not discriminate against the complainant on grounds prohibited by the *Canadian Human Rights Act*. However, the Committee noted that the Service could have been more sensitive in the manner in which it delivered its decision of not being able to accommodate the complainant with part-time employment.

The complainant had been working a limited number of hours per week because of disabilities. The Service required the duties of the complainant's position to be performed on a full-time basis. To have those duties performed on a part-time basis would have caused undue hardship to the Service. The Committee concluded that the Service did not fail in its duty to accommodate the complainant, and did not discriminate against the complainant on grounds prohibited by the *Canadian Human Rights Act*. However, the Committee noted that the Service could have been more sensitive in the manner in which it delivered its decision of not being able to accommodate the complainant with part-time employment.

Further, the Committee determined that—given the national security concerns associated with the investigation of the complaint—neither the Canadian Human Rights Commission nor the Canadian Human Rights Tribunal could conduct a meaningful investigation or hearing concerning the complaint.

Accordingly, the Committee recommended that the Canadian Human Rights Commission dismiss the complaint.

REPORT: SECTION 41 ("ANY ACT OR THING")

The Committee reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act*, which states that any person may make a complaint about "any act or thing done by the Service."

The complaint alleged that a Service employee had improperly conducted immigration security screening interviews with the complainant. After holding a hearing and reviewing the evidence, SIRC concluded that the complainant had not presented any evidence that would suggest the interviews were improperly conducted.

The Committee determined that due in part, to the fact that the complainant's first language was neither French nor English, the complainant suffered from misapprehension or confusion during the immigration screening process as a result of correspondence from CIC.

REPORT: SECTION 42 (DENIAL OF SECURITY CLEARANCE)

SIRC reported a decision on a complaint pursuant to Section 42 of the *CSIS Act*, concerning a denial of security clearance.

The complainant applied for employment with an agency of the federal government, which denied the applicant the required security clearance based on information given to it by CSIS. The complainant contested the denial of the security clearance by filing a complaint with SIRC.

The decision of the deputy head to deny the security clearance was reasonable and the Committee recommended that the decision be upheld.

The complainant was seeking a Top Secret security clearance. According to the *Government Security Policy*, a Top Secret security clearance may not be granted where there are reasonable grounds to doubt the applicant's loyalty to Canada or reliability as it relates to loyalty.

The Committee concluded that there were reasonable grounds to believe that the complainant may have engaged in intelligence collection activities on behalf of a foreign state, and appeared to have maintained regular contact with foreign representatives, who may have been involved in intelligence collection activities. Therefore, the decision of the deputy head to deny the security clearance was reasonable and the Committee recommended that the decision be upheld.

Complaints About CSIS Activities Under Section 41

Under Section 41 of the *CSIS Act*, SIRC must investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before SIRC investigates, two conditions must be met:

1. the complainant must first have complained to the Director of CSIS and not received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and

2. the Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith. Under Section 41(2) of the *Act*, the Committee cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Staff Relations Act*.

Complaints About CSIS Activities Under Section 42

With respect to decisions by federal deputy heads to deny security clearances, Section 42 of the *CSIS Act* says the Review Committee shall investigate complaints from:

1. any person refused federal employment because of the denial of a security clearance;

2. any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and

3. anyone refused a contract to supply goods or services to the government for the same reason.

A complaint under Section 42 of the *Act* must be filed within 30 days of the denial of the security clearance. SIRC can extend this period if valid reasons are presented.

Referrals Under the *Canadian Human Rights Act*

In the event that the Canadian Human Rights Commission receives—under Subsection 45 (2) of the *Canadian Human Rights Act*—written notice from a Minister of the Crown that the practice to which a complaint relates was based on considerations relating to national security, the Commission may dismiss the complaint or refer the matter to SIRC. On receipt of such a referral, the Committee carries out an investigation and after consulting with the Director of CSIS pursuant to Section 55 of the *CSIS Act*, reports its findings to the Commission, the Minister who referred the complaint, and the complainant.

C. Section 54 Report to the Minister of Public Safety and Emergency Preparedness

Pursuant to Section 54 of the *CSIS Act*, SIRC may report to the Minister of Public Safety and Emergency Preparedness on any matter relating to the performance and functions of the Service.

In fall 2003, SIRC determined that the events involving Maher Arar were sufficiently important to warrant a special report of this nature. While the report's specific findings cannot be discussed as the matter remains the subject of an ongoing inquiry by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor Commission), this case illustrates the difficult dilemma often faced by the Committee. Because of SIRC's legal obligation to protect both national security and privacy concerns, it is often difficult to convey the thoroughness or complexity of SIRC reviews, or provide the details that might help to substantiate its findings and recommendations.

SIRC was unfairly criticized when the government released a heavily redacted version without consulting the Committee. SIRC has stated publicly that it would have "no objection" if a summary of its classified report is released by the O'Connor Commission, once its own investigation is completed.

SIRC launched its Section 54 review months before the Commission of Inquiry was established. The Committee reviewed all material available to it under the *CSIS Act*, and provided its findings to the Minister in May 2004. Although the entire report was shared with the Commission, SIRC was unfairly criticized when the government released a heavily redacted version without consulting the Committee. SIRC has stated publicly that it would have "no objection" if a summary of its classified report is released by the O'Connor Commission, once its own investigation is completed.

As noted, SIRC may review only the activities of CSIS. However, in carrying out its review, SIRC identified a number of issues that appeared to warrant examination by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar:

- the role of other federal departments and agencies in Arar's rendition to Jordan by U.S. authorities;
- Arar's subsequent detention and interrogation in Syria;
- whether CSIS information was included in RCMP files that were shared with American authorities; and
- how the United States came into possession of Arar's 1998 rental-lease agreement.

SIRC concluded that the O'Connor Commission might also wish to comment upon the protections offered to Canadian citizens by the new Consular Understanding between Canada and the United States, announced by Canada's Foreign Affairs Minister on January 13, 2004.

Section 2

CSIS Accountability Mechanisms

CSIS Accountability Mechanisms

A. Reporting Requirements

At least once a year, the Director of CSIS is required to submit to the Minister a report on the operational activities of the Service in accordance with Section 33(1) of the *CSIS Act*, which in turn is given to the Inspector General. After receiving the Director's report, the Inspector General is required to submit to the Minister a certificate stating the extent to which she or he is satisfied with the report, and to inform the Minister of any unauthorized activities or any unreasonable or unnecessary use of powers. The Minister is then required to submit the Director's report and the Inspector General's Certificate to SIRC.

Under Section 38(a)(i) of the *CSIS Act*, SIRC is required to review the Director's report and the Inspector General's certificate. SIRC's examination of the Director's report and Inspector General's certificate has proven helpful in identifying potential areas for future research and review. The Committee also uses the Director's report and the Inspector General's certificate to make yearly comparisons of CSIS activities and to monitor the performance of existing and new programs and sectors.

This section of SIRC's annual report reviews the Director's report, the Inspector General's certificate and summarizes other CSIS reporting requirements.

CERTIFICATE OF THE INSPECTOR GENERAL FOR 2004

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG functions as the Minister's internal auditor of CSIS, reviewing the Service's operations. The Inspector General is responsible to the Deputy Minister of Public Safety and Emergency Preparedness, providing an independent means of assurance that CSIS is complying with the *CSIS Act*, Ministerial Direction and operational policy.

The certificate issued in November 2004 was the first to be issued by the current IG, who was appointed in December 2003. SIRC noted that the IG has adopted the validation process established by her predecessor, which consists of the review of select information and intelligence collected and retained by the Service. It also includes an examination of branch accountability reports and the "facting" on which they are based.

The IG also chose to review:

- a selected sample of warrants, targets and human-source case management;
- a sample of CSIS's foreign arrangements;
- CSIS's assistance to the Departments of Foreign Affairs and National Defence in the collection of foreign intelligence in Canada; and
- CSIS's involvement in the Integrated National Security Assessment Centre, the security certificate process, and a counter-intelligence operation.

In the certificate, it was noted that the Director of CSIS also reported five incidents of non-compliance with operational policy for 2003–2004. The IG looked into each of these incidents and found that appropriate action had been taken in each case.

In this year's certificate, the Inspector General reported to the Minister that she was "as satisfied as she could be" with the Director's annual report on the Service's operational activities. She concluded that the Service had exercised its duties and functions with a commendable degree of professionalism.

CSIS DIRECTOR'S ANNUAL OPERATIONAL REPORT 2003–2004

Every year, as noted, the Director of CSIS prepares for the Minister of Public Safety and Emergency Preparedness a report on the operational activities of the Service, which is sent to SIRC for review. The report outlines the achievements realized and challenges encountered by the Service in the preceding period.

In the 2003–2004 edition of this report, the Director noted that CSIS resources have expanded since the September 11th attacks, and also addressed specific challenges in meeting the demands of the current threat environment. The Director noted that perhaps the greatest challenge is the international and transnational nature of threats to the security of Canada, which have broadened the platform of Service operations. He noted that, increasingly, the most effective means of acquiring threat-related information is to obtain it offshore. The Director also highlighted an increasing need for joint operations and the Service's efforts to build relationships for greater liaison capacity with domestic partners and foreign allies.

i. Counter Terrorism

The report noted that the Service's highest priorities continue to be public safety and safeguarding against terrorist attacks occurring in or originating from Canada. The report described the priority counter-terrorism (CT) investigation, Sunni Islamic extremism. Other ongoing CT investigations were summarized, including the initiation of a new investigation into the potential for violence related to instability and conflict

in a specific country. A reduced threat level led the Service to terminate one particular investigation. The Director also described targeting authorities for certain terrorist organizations, mainly with respect to fundraising and support activities being undertaken in Canada.

The activities of the Terrorist Financing Unit (TFU) within the Counter Terrorism Branch were also summarized. This unit provides the Government of Canada with intelligence on the nature and extent of terrorist financing networks in Canada. As of April 1, 2004, there were 24 organizations listed as a result of the terrorist entity listing process.

ii. Counter Proliferation

The Director's report outlined ongoing Counter Proliferation (CP) investigations, including state sponsored terrorism as well as the foreign interference and espionage activities of specific foreign governments. The CP Branch was also responsible for Counter Proliferation Operations, the Foreign Intelligence and Assessments section, and the Integrated National Security Assessment Centre, which was scheduled to be reorganized into the Integrated Threat Assessment Centre, under the direction of the Prime Minister's National Security Advisor.

CSIS's Counter Proliferation Branch investigated the continuing threat posed by the proliferation of weapons of mass destruction. The Director reported that the international nature of the threat meant that many of the Service's investigations in the counter-proliferation area required close cooperation with allied intelligence services.

iii. Threat Assessment Centre

Also featured in the report were the activities of the CP Branch's Threat Assessment Centre, which is responsible for the Threat Assessment Unit (TAU) among others. The TAU is responsible for analyzing potential threats to Canadian interests at home or abroad, as well as threats to foreign interests and internationally protected persons located or travelling in Canada. The report noted the introduction of defined threat levels and the creation of a working group within the TAU in Ottawa.

The Director reported that the CP Branch worked closely with Citizenship and Immigration Canada (CIC), the Canada Border Services Agency and the then-Canada Customs and Revenue Agency (CCRA) to deny or monitor the entry to Canada of individuals who might pose a threat to the security of Canada.

The report also detailed the Branch's activities in support of efforts to remove two individuals from Canada, and in providing litigation support in two other cases in which the assessment of danger is ongoing.

iv. Integrated National Security Assessment Centre

During 2003–2004, the CSIS Director also reported to the Minister on the work of the Integrated National Security Assessment Centre (INSAC), which became operational in February 2003. This group comprised federal agencies with various responsibilities in the national security area, and allowed participants to access, share, analyze and disseminate information and intelligence. INSAC's efforts focussed on specific subjects of immediate and near-term interest. The Centre has since been replaced by the Integrated Threat Assessment Centre (ITAC), under the policy direction of the Prime Minister's National Security Advisor. Functional, day-to-day responsibility for the ITAC lies with the Director, CSIS.

v. Counter Intelligence

The report highlighted the work of the Counter Intelligence (CI) Branch. This branch investigates the activities of specific countries that dedicate significant effort to the clandestine collection of information to further their political, military and economic intelligence goals, as well as interference in expatriate communities in Canada. The report outlined the activities of certain countries and noted additional countries that were the subject of CI investigations.

vi. Human Source Program

The Director's report also detailed the Service's human source program, providing information on the number of human sources and the cost of the program. The Director's exercise of delegated authority for certain source activities was also reported, along with instances of Ministerial approval required in specific circumstances.

vii. Other Key Points

The Director noted that the creation of the Canada Border Services Agency was one of the most significant developments for the Security Screening Immigration Program during the reporting period. The report outlined the activities in the Security Screening Branch's four components that comprise immigration screening.

CSIS provides security assessments for all federal government departments (excluding the RCMP), and has several site-access programs, a Provincial Government Program and reciprocal agreements with foreign agencies. Specific activities in relation to each of these programs were outlined in the report.

During the reporting period, CSIS managed 16 Memoranda of Understanding (MOU) with federal government departments and agencies and MOUs with eight provinces. The Director reported no significant issues in relation to these arrangements.

The report also outlined Service activities concerning the 247 foreign arrangements in place as of March 31, 2004, including 13 new arrangements and the consolidation of three existing arrangements. Also of note, the Director reported on the efforts and challenges facing the Scientific and Technical Services Branch.

UNLAWFUL CONDUCT BY CSIS

Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director's opinion, a CSIS employee may have acted unlawfully in performing his or her duties and functions. The Minister, in turn, must send the report with her comments to the Attorney General of Canada and to SIRC.

In 2004–2005, the Service reported no such activity to the Minister.

SECTION 2(d) INVESTIGATIONS

The Service is authorized to collect, analyze and retain information and intelligence on activities that may be suspected of constituting a threat to the security of Canada. Section 2(d) of the *CSIS Act* defines a threat to include: activities directed towards undermining by covert unlawful acts, or intended to lead to the destruction or overthrow by violence of, the system of government in Canada. The Minister of Public Safety and Emergency Preparedness must authorize CSIS investigations of these threats. The Service reported that in 2004–2005, the Minister did not approve any investigations under Subsection 2(d).

DISCLOSURES OF INFORMATION IN THE PUBLIC OR NATIONAL INTEREST

CSIS may disclose information it has obtained in the performance of its duties and functions only in accordance with the specific conditions set out in Section 19 of the *CSIS Act*. Section 19(2)(d) of the *Act* authorizes the Minister to approve disclosures to individuals identified in the section, where such a disclosure would be in the public interest and that interest outweighs the resulting invasion of privacy.

The Service reported to SIRC that no such disclosures were approved in 2004–2005.

Disclosure of Information by CSIS

Section 19 of the *CSIS Act* sets out four situations in which the Service may disclose information obtained in the performance of its duties and functions. These situations are defined under Subsection 19(2) as follows:

(a) information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, the Minister of Public Safety and Emergency Preparedness or the Attorney General of the province in question;

(b) information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;

(c) information related to the defence of Canada may be disclosed to the Minister of National Defence; and

(d) information that, in the opinion of the Minister, is essential to the public interest may be disclosed to any minister of the Crown or employee of the Public Service of Canada. The Director of CSIS must submit a report to SIRC with respect to disclosures made in the public interest.

B. Policy and Governance Framework

ANNUAL NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

Background

Pursuant to Subsection 6(2) of the *CSIS Act*, the Minister of Public Safety and Emergency Preparedness issues annual National Requirements for Security Intelligence to provide general direction to CSIS in its collection, analysis and advisory responsibilities as detailed in the *CSIS Act*.

The 2004–2005 National Requirements direct the Service to continue to maintain a flexible forewarning capability and meet Canada's evolving security intelligence needs by relying on risk management. The Minister notes that this approach will allow the Service to concentrate its resources on the foremost threats, while retaining the ability to respond to emerging issues in a timely fashion. CSIS is directed to focus on security intelligence needs with respect to the security of Canada as set out in Section 2 of the *CSIS Act*.

For 2004–2005, the Minister has directed CSIS to pursue the enumerated priorities in accordance with its mandate, including:

- safeguarding against the possibility of a terrorist attack occurring in or originating in Canada or affecting Canadian citizens or assets abroad;
- assessing the potential for attacks involving weapons of mass destruction;
- providing advice on Canada's economic security;
- safeguarding confidential Government of Canada information; and
- advising on threats to critical infrastructure.

In the 2004–2005 National Requirements, the Minister notes that today's threat environment is increasingly international and transnational in nature—intelligence work cannot be suspended at the Canadian border. CSIS is therefore directed to pursue foreign sources of threat-related information. It is also directed to support the establishment and operation of an Integrated Threat Assessment Centre (ITAC), as part of the Government of Canada's commitment to enhanced information-sharing and to ensure the timely distribution of ITAC assessments. ITAC will replace CSIS's Integrated National Security Assessment Centre (INSAC).

The National Requirements acknowledge the demonstrated willingness of individuals, groups and states to use violence in support of political, religious, ideological or territorial objectives. The Minister notes that preferred target venues include locations that will yield maximum destruction and casualties. Further, the National Requirements acknowledge that Canada's response to terrorist activities has raised Canada's profile with terrorist actors and proponents.

As has been previously acknowledged, a significant portion of the world's terrorist groups are represented in Canada. The Minister notes that these groups engage in such activities as fundraising, lobbying, document fraud, planning and staging of terrorist acts, manipulation of émigré communities, facilitation to and from the United States, and the procurement of dual-use materials.

To a lesser extent, Canada also faces domestic issues that may lead to extremist acts or threats of serious violence. Therefore, CSIS is directed by the Minister to investigate and advise the Government of Canada about threats arising from:

- religious extremism;
- state-sponsored terrorism;
- secessionist violence;
- domestic extremism; and
- terrorist financing.

The Minister has also directed the Service to continue to conduct research and analysis in support of the terrorist entity listing process; to support Department of National Defence deployments; to increase its liaison capacity with foreign partners; and to work towards the prosecution, deportation and denial of safe haven to members of terrorist organizations in cooperation with other federal departments and agencies.

> The Minister notes that today's threat environment is increasingly international and transnational in nature—intelligence work cannot be suspended at the Canadian border.

CSIS is directed by the Minister to continue to identify countries and groups engaged in developing weapons of mass destruction (WMD) and other weapons proliferation programs and to support Canada's obligations to stem the acquisition of WMD and other forms of proliferation, through the provision of relevant intelligence. The Minister also notes the activities of countries that collect information in and about Canada in support of their military, political and economic needs. CSIS is directed to investigate these threats, including foreign-influenced activities; transnational criminal activities; clandestine or coercive efforts by foreign governments to gain access to intelligence, proprietary information or technology; and attempts to steal, alter or destroy information or critical infrastructures.

The National Requirements note that CSIS's security assessments, screening investigations and security advice on immigration and citizenship matters are an important part of the Service's mandate. CSIS is directed to continue advising the Government of Canada on these matters and to provide security assessments in relation to citizenship and immigration processes, airports, land borders, marine security, Parliamentary precincts, nuclear power stations, restricted areas at special events, Order-in-Council appointments, and certain provincial governments.

Finally, CSIS is directed to continue to provide the Government of Canada with relevant, comprehensive and policy-neutral intelligence assessments and to keep pace with the rapid development of new technologies. In addition to upgrading technical equipment and information systems, the Service is directed to collaborate with the RCMP, the Department of Justice, Industry Canada, the Department of Public Safety and Emergency Preparedness Canada and other departments and agencies to prepare policy and legislation ensuring that Canada's laws keep pace with evolving technologies.

MINISTERIAL DIRECTION

Under Section 6(2) of the *CSIS Act*, the Minister may issue directions governing CSIS's activities and investigations. The Ministerial Direction on National Requirements for Security Intelligence for 2004–2005 is described in the section above. No other directions were issued in the year under review.

GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

Under Section 8(4) of the *CSIS Act*, the Governor-in-Council may issue regulations to the Service concerning the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees. No such regulations were issued in 2004–2005.

CHANGES IN CSIS OPERATIONAL POLICY

CSIS Operational Policy sets out the parameters and rules governing the entire range of the Service's operational activities. The Operational Policy is regularly updated to conform to changes in legislation and Ministerial Direction. All changes to this policy are reviewed by the Committee to ensure that they conform with law and Ministerial Direction. Applicable operational policies are also reviewed and CSIS compliance with those policies assessed in the course of each of the reviews carried out by SIRC.

The Service reported to SIRC on the new operational policies implemented in 2004–2005, together with new policies under development and revisions to existing policies. CSIS noted that the major factors influencing these developments included changes in existing legislation, passage of new legislation and changes in operational methodology. Revised policies in 2004–2005 covered such subjects as Section 12 warrant acquisitions and caveats used in the disclosure of operational information and intelligence.

The Service reported to SIRC on the new operational policies implemented in 2004–2005, together with new policies under development and revisions to existing policies.

Two policies were under development during fiscal year 2004–2005. The first concerned the acquisition of production orders and the second addressed certain operational reporting. The Service also reported that a number of existing policies were under revision during the reporting period. These addressed subjects such as targeting, foreign liaison and cooperation, warrant powers and approvals, cooperation with Citizenship and Immigration Canada and the Canada Border Services Agency, and operational reporting.

In addition, SIRC obtained an update from the Service on the status of policies that were under development at the end of fiscal year 2003–2004. Several of these have since been implemented. CSIS reported that one policy project was still ongoing, as it required considerable consultation and was affected by the restructuring of certain government departments. A second policy project, intended to revise certain information disclosure procedures, was on hold at the end of fiscal year 2004–2005.

C. CSIS Operational Activities

COUNTER PROLIFERATION

The Counter Proliferation (CP) Branch collects information related to biological, chemical and nuclear weapons development programs of foreign governments. It also investigates state sponsorship of terrorism.

This is a relatively new branch, created in 2002. As such, in 2002–2003, SIRC committed to undertake in-depth reviews of this group in future years. In 2003–2004, the Committee undertook a review of the Service's investigation of the threat to Canadian security posed by one country's weapons of mass destruction (WMD) program (*see SIRC study # 2003-04*). In 2004–2005, SIRC reviewed a CP Branch investigation of actions by another country regarding WMD.

In 2004–2005, the CP Branch produced 406 of these reports—a significant reduction from 650 in the previous fiscal year.

The branch's Threat Assessment Unit produces threat assessment reports on a wide range of topics. In 2004–2005, the CP Branch produced 406 of these reports—a significant reduction from 650 in the previous fiscal year. CSIS reported that the reduction was attributable to a number of factors, including revisions to reporting practices, changes in staffing and the creation of the Integrated Threat Assessment Centre (ITAC) which, in 2004, replaced the branch's Integrated National Security Assessment Centre.

The Service also briefed SIRC on the creation of a new unit that manages the Service's investigations of certain foreign state-driven weapons of mass destruction (WMD) programs and proliferation-related activities.

As reported in previous SIRC annual reports, one of the priorities of CP Branch in 2004–2005 was the investigation of efforts by a certain country to advance its WMD programs and capabilities.

The Branch also expanded its intelligence collection regarding states that sponsor terrorism, as well as the terrorist groups that benefit from that support. The CP Branch reported to SIRC that it had succeeded in identifying, recruiting and directing human sources to report on these matters.

The Branch provided SIRC with information on the role played by CSIS in connection with the November 2004 visit to Canada by United States President George W. Bush. The Branch worked closely with other Service branches and government partners responsible for security during this event. The Threat Assessment Unit prepared numerous threat assessment reports, and the CP Branch seconded staff to the RCMP National Operations Centre for the duration of the visit.

The Service also reported on information provided to a government agency pertaining to efforts of a particular country to acquire restricted technology. Based on information from both domestic sources and a foreign intelligence agency, CSIS also learned of an institution operating in Canada which had possible links to a terrorist organization.

COUNTER TERRORISM

The role of the Counter Terrorism (CT) Branch is to advise the Government of Canada on emerging threats of serious violence that could affect the safety and security of Canadians and of Canada's allies. These threats could originate in Canada or abroad.

As reported in SIRC's previous three annual reports, Sunni Islamic extremism remained the major focus of the Counter Terrorism Branch's operational activities. It undertook certain restructuring to respond to the fluidity of this priority. Additional reassignments at the supervisory level were also implemented within the branch in 2004–2005.

It also reported on a new and growing extremist threat in Canada and other Western democracies, in which targets are in their twenties, technologically savvy and completely westernized.

A new and growing extremist threat in Canada and other Western democracies, in which targets are in their twenties, technologically savvy and completely westernized.

The CT Branch also reported on support to the RCMP and a foreign intelligence service. A total of 137 Section 19 disclosure letters were issued by the Branch in 2004–2005. This section of the *CSIS Act* authorizes the Service to disclose information obtained in the performance of its duties and functions to Canadian law enforcement, diplomatic and defence personnel. The Branch also provided SIRC with details regarding the total number of individual and organizational targets that were the subject of ongoing investigations during the year under review.

In 2004–2005, the Committee reviewed CSIS counter-terrorism investigations as well as the Service's advice to the government concerning terrorist financing. The results of these studies are presented in this report. SIRC will continue to undertake reviews of CSIS's counter-terrorism investigations in 2005–2006.

COUNTER INTELLIGENCE

The Counter Intelligence (CI) Branch investigates threats to national security from the hostile intelligence activities of foreign governments. These activities may include espionage, foreign-influenced activity, transnational crime and threats to Canada's social, political, and economic infrastructure.

The Service reports that there have been no structural changes to the Branch and the 2005–2006 Annual Plan has made no changes to the priorities as outlined in the annual plan for the previous year. The Service notes that the espionage activities of CI's targets continue to become more complex and sophisticated. CSIS reported to SIRC on the measures taken to address these challenges. The CI Branch continues to place great importance on human source recruitment to maximize its operational effectiveness.

During the year under review, the CI Branch did not issue any Section 19 disclosure letters or advisory letters. The Branch informed SIRC of the number of targets and level of targeting authority; these include individual, organization and issue-based targets.

RESEARCH, ANALYSIS AND PRODUCTION (RAP) BRANCH

RAP is responsible for producing security intelligence assessments to support the Service's operations and the Government of Canada's decision-making in relation to threats to national security. Given the nature of the today's security environment and the immediacy of information, RAP must ensure that the information provided to decisionmakers is accurate and timely.

> "The involvement of this many of RAP's resources resulted in successfully satisfying the legislative requirements of the listing process; however, it did affect the ability of RAP to maintain its 'normal' research and production responsibilities."

In fiscal year 2004–2005, RAP chose to focus on the production of strategic and operational analyses of current threats and emerging issues. The *Intelligence Briefs, Reports* and *Studies* remain core RAP documents, and are distributed widely throughout the security intelligence community, including SIRC.

In 2004–2005, responsibility for two programs was redirected to RAP. This branch is now the central point for the management

of all the information received from one of the Service's major allies and for the subsequent dissemination of this information on behalf of the CT, CI and CP branches.

The Research, Analysis and Production Branch took on responsibility for the Terrorist-Entity Listing Process this year, at the time of the two-year review of the listings process. As indicated in SIRC study # 2004-03, RAP described their involvement in the first two-year review of the terrorist list as a "major project." The review process involved five research librarians from the Information Centre, twelve RAP analysts, and four lawyers. RAP estimates that approximately ten days were necessary to research and write a two-year review SIR for each of the 35 entities listed. RAP noted that "the involvement of this many of RAP's resources resulted in successfully satisfying the legislative requirements of the listing process; however, it did affect the ability of RAP to maintain its 'normal' research and production responsibilities."

Finally, RAP must report Section 19 disclosures. RAP discloses information to the RCMP under Section 19(2)(a), of which there were 155 disclosures in 2004–2005. The CT, CP and CI Branches reported to SIRC on their Section 19(2)(a) disclosures to law enforcement agencies. As for Section 19(2)(b) disclosures to Foreign Affairs Canada, the Service reported that there were 673 in 2004–2005. Finally, there were 384 disclosures to the Department of National Defence by RAP under Section 19(2)(c).

RAP Intelligence Products

Research, Analysis and Production Branch (RAP) intelligence products originate from a number of sources and are produced either on the recommendation of an analyst, at the direction of a RAP supervisor or manager, or CSIS senior management, or at the request of an operational branch, region, or external client. They are defined as follows:

CSIS Study

An analytical product resulting from extensive in-depth research encompassing all elements relating to a threat to the security of Canada. The intention is to provide a reference document for CSIS operational branches and/or external clients. A CSIS study contains an executive summary, is not limited in length, and is usually classified.

CSIS Report

A concise analytical product that is the result of research on a current security threat pertaining to the Service mandate. The aim is to explain the nature of the threat in some detail to internal and external readers. A CSIS report is usually classified and is up to eight pages long.

RAP Intelligence Products *(continued)*

CSIS Intelligence Brief (CIB)

A concise analytical product designed to provide internal and external clients with an analysis of a current threat or an emerging issue relating to the Service mandate. A CIB is usually classified and up to three pages in length.

Profiler

Intended to provide well-focussed information on countries, individuals or groups of interest to the Service. The document is essentially a tool for Service investigators and operational analysts. A Profiler is usually classified "CSIS Eyes Only" and is not released externally without prior removal of sensitive information and consultation with operational branches. Profilers do not exceed three pages. Some Profilers are unclassified but carry the added caveat "For Official Use Only."

Fact Sheet

Designed to provide information about the past or current organizational structure of foreign intelligence and security services. It identifies the collection priorities they may be engaged in or relating to Canada. This product is also used to provide information on specific issues such as organized crime groups and oligarchs, and countries of proliferation concern. Sheets are restricted to CSIS employees only.

Commentary

Commentary, written by individuals hired on contract, provides information on a wide range of subjects that may have an influence on the security of Canada. These are strategic documents with wide domestic and international distribution and are unclassified.

Special Report

This is a classified document intended for a very narrow or specific readership and is usually the result of an event or an action request by a government department.

SECURITY SCREENING

Section 13(1) of the *CSIS Act* authorizes the Service to provide security assessments to federal government institutions. The *Act* defines a security assessment in Section 2 as "an appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual." The Service may also, under Sections 13(2) and (3), enter into

arrangements to provide assessments to provincial government institutions or police forces, or to foreign governments and international institutions.

In 2004–2005, CSIS received a total of 101,097 government security clearance and "site-access" assessment requests. This represents a significant increase over the 74,835 requests processed in 2003–2004.

Under Sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency to assist in processing refugee, immigration and citizenship applications. The Service's advice in these cases is based on the classes of individuals deemed inadmissible under the security-related criteria of the *Immigration and Refugee Protection Act*. CSIS also provides security assessments to CIC to assist in screening citizenship applications, pursuant to Section 19 of the *Citizenship Act*.

Table 2
Turnaround Times for Security Screening of Refugee Claimants and Immigration Applicants (2004–2005)

CSIS Security Screening Programs	Median[16] Turnaround (Calendar Days)		
	Non-adverse Advice	Information Briefs	Inadmissible Briefs
Front-end screening of refugees	27	336	248
Applications for permanent residence within Canada—refugee determination program	56	515	527
Applications for permanent residence within Canada—immigration program	44	511	333
Applications for permanent residence from the USA	150	599	642
Applications for permanent residence from outside Canada (excluding USA)	7	531	236

16. In this section of the annual report, SIRC refers to the Service's *median* turnaround times for processing screening requests rather than average or *mean* times. The Committee believes this represents more accurately the typical processing times by mitigating the impact of unusually short or lengthy processing times.

In 2004–2005, CSIS received a total of 101,097 government security clearance and "site-access" assessment requests. This represents a significant increase over the 74,835 requests processed in 2003–2004. Also of note during 2004–2005, the Service issued 39 information briefs and three recommendations for denial of government security clearances. For the same period, the Service received a total of 254,364 requests for immigration, refugee, front-end screening and citizenship screening.

There was one structural change within the Branch during the past fiscal year, to process site-access requests. The Branch reported that there were no changes to security screening priorities as outlined in their 2004–2005 annual plan.

Security Clearances

The Service reported that it received 36,519 requests for new or updated security clearances—down slightly from 37,508 during the previous fiscal year. In 2004–2005, there was a significant increase in the turnaround times for Level I (Confidential) and II (Secret) security assessments for the Department of National Defence (DND), and an improvement in the turnaround time for DND on Level III (Top Secret) clearances. For the balance of federal departments and agencies, there was a small increase in the median turnaround for Level I and II clearances, with an improvement to Level III turnaround times.

The Service reported that it received 36,519 requests for new or updated security clearances—down slightly from 37,508 during the previous fiscal year.

The median turnaround times for the Service to provide its assessments to government clients can be found in Table 3 below.

Table 3
Turnaround Times for Security Screening of Government Clients

Category	Level	Median Number of Calendar Days	
		2003–2004	2004–2005
DND	I (Confidential)	20	49
	II (Secret)	18	63
	III (Top Secret)	96	70
Other departments and agencies	I (Confidential)	7	12
	II (Secret)	11	14
	III (Top Secret)	82	69

Site-Access Programs

The Service received a total of 64,578 site-access requests in 2004–2005. This is an increase compared to the 28,822 requests received in 2003–2004. Of these, the Service received 31,086 requests under the *Airport Restricted Access Area Clearance Program*. The median turnaround time for the Service's response to these requests was 24 calendar days.

Included in the 64,578 processed requests were 7,857 requests by nuclear power facilities and the Parliamentary Precinct (which includes all facilities controlled by the Parliament of Canada). The median turnaround time for a response to these site-access requests was one calendar day. The balance of the requests (i.e., those received from other government departments) were processed in one calendar day.

Table 4
Site-Access Programs

Program	Number of Site-Access Requests Processed	Median Turnaround Time (Calendar Days)
Parliamentary Precinct Program	1,110	1
Airport Restricted Area Program	31,086	24
Nuclear facilities	6,747	1
Other government departments	25,635	1

Screening on Behalf of Foreign Agencies

The Service may enter into reciprocal arrangements with foreign agencies to provide security assessments on Canadians and other individuals who have resided in Canada. Under these arrangements, the Service does not make recommendations to foreign agencies to deny security clearances, but simply reports its findings concerning the individual(s).

In 2004–2005, the Service concluded 869 screening requests on behalf of foreign agencies—down from the 1,208 checks concluded in 2003–2004. Field investigations were conducted in 151 of these screening requests.

Security Screening for the Refugee Claimants and Immigration Applicants

In 2004–2005, CSIS received 97,761 requests for security screening of immigration and refugee applicants—a decrease of 3,529 applications from the previous fiscal year. The Service provided immigration officials with a total of 232 information briefs and 150 inadmissible briefs. In the previous fiscal year, CSIS produced 221 information briefs and 99 inadmissible briefs.

In 2004–2005, CSIS received 97,761 requests for security screening of immigration and refugee applicants—a decrease of 3,529 applications from the previous fiscal year.

In 2004–2005 the Service also provided 16 incidental letters and 55 updates to briefs previously issued to CIC. A description of the types of advice CSIS provides to CIC can be found in the inset on page 64.

Security screening of refugee and immigration applicants is carried out under the three main programs listed in Table 5 below.

Table 5
Security Screening of Refugee Claimants and Immigration Applicants (2004–2005)

CSIS Security Screening Programs	Requests Received	Information Briefs	Inadmissible Briefs
Front-end screening of refugees	22,871	115	69
Applications for permanent residence within Canada	38,628	84	65
Applications for permanent residence from outside Canada (including SLO referrals)	36,262	33	16
Total	**97,761**	**232**	**150**

Front-End Screening of Refugee Claimants

The Front-End Screening (FES) Program, implemented by the Government of Canada in November 2001, identifies potential security concerns about refugee claimants in Canada as early as possible in the refugee determination process. For 2004–2005, the Service reported receiving 22,871 applications under this program. During the

same period, the Service provided advice on 22,227 cases—including 115 information briefs and 69 inadmissible briefs.

For 2004–2005, the Service reported receiving 22,871 applications under the Front-End Screening Program.

Under the FES Program, the median turnaround time for the Service to issue non-adverse advice was 27 days. Median turnaround times were 336 days for information briefs and 248 days for inadmissible briefs. This represents a small increase over last year's numbers of 332 days for information briefs and 214 days for inadmissible briefs.

Applications for Permanent Residence from Within Canada

The Service is responsible for security screening all persons who apply for permanent residence status from within Canada. In 2004–2005, the Service received 38,628 requests—24,389 under Canada's immigration program and 14,239 through the refugee determination program.

The median turnaround times for the Service to provide its advice in these cases varied considerably in 2004, depending on whether the Service received the request in hard copy or via Electronic Data Exchange (EDE). The Service noted that electronic exchanges are already well established for Canada's immigration program—with the exception of overseas immigration and vetting of visa applications. Ninety-five percent of inland Canada immigration applications were conducted electronically (EDE). For 2004–2005, the median turnaround time for hard-copy applications was 33 days, and 45 days for EDE applications.

Applications for Permanent Residence from Outside Canada

For permanent residence applications originating outside Canada or the United States, the Service shares responsibility for security screening with immigration officials at Canadian missions abroad. In such cases, CSIS only becomes involved in the process when they receive a request from the Immigration Program Manager. This process allows the Service to focus on higher-risk cases.

During this review period, the Service received 5,408 requests to provide screening advice for applications submitted to Canadian immigration offices in the United States.

During this review period, the Service received 5,408 requests to provide screening advice for applications submitted to Canadian immigration offices in the

United States. For these applications, the median turnaround time was 25 calendar days for electronic (EDE) applications and 288 days for hard-copy applications.

Forty-four percent of immigration applications originating in the United States were submitted electronically. The median turnaround time for immigration security screening cases that resulted in a *Notice of Assessment—Checked on the Basis of Information Supplied* or *No Reportable Trace* was 150 days.

For applications from outside Canada, other than the United States, the Service concluded 26,430 requests. Eighty-three percent of these applications were managed electronically by EDE. The median turnaround time for hard-copy applications was 38 calendar days—electronic applications took six calendar days. In addition, the Service's Security Liaison Officers were consulted on 4,593 cases. The Service issued 17 information briefs and 11 inadmissible briefs. The median turnaround times were 531 days for information briefs, 236 days for inadmissible briefs and seven days for non-adverse advice.

CSIS's advice to Citizenship and Immigration Canada (CIC)

The Service's security screening assessments are provided to CIC in one of four forms:

- *Notice of Assessment—Checked on the Basis of Information Supplied and/or No Reportable Trace:* This report is given to CIC when the Service has no adverse information on the applicant.

- *Inadmissible brief:* Advice provided when the Service has concluded, based on information available to it, that an applicant meets the inadmissibility criteria outlined in the security provisions of the *IRPA*.

- *Information brief:* Advice provided by CSIS when it has information that the applicant is or was involved in activities as described in the security provisions of the *IRPA*, but that the Service is of the opinion the applicant does not fall into the class of persons deemed to be inadmissible under the *Act*.

- *Incidental letter:* Provided to CIC when the Service has information that the applicant is or was involved in non-security-related activities described in the *IRPA* (e.g., war crimes or organized criminal activity) or any other matter of relevance to the performance of duty by the Minister of Citizenship and Immigration, as set out in Section 14(b) of the *CSIS Act*.

Foreign Liaison and Visits (FLV) Branch

The Foreign Liaison and Visits (FLV) Branch is responsible for the Service's liaison with foreign agencies. It uses liaison channels to exchange information on threats to the security of Canada.

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with foreign states—including foreign governments or international organizations of states or institutions thereof—for the purpose of performing its duties and functions. While Ministerial Direction and Service operational policy outline the principles regarding the establishment and management of such arrangements, the scope of a foreign arrangement determines the nature and extent of the Service's cooperation and exchanges with a foreign agency. The scope also identifies the specific type of information sharing that can occur.

At the end of fiscal year 2004–2005, the Service had 257 foreign arrangements with 143 countries. During that period, the Service received Ministerial approval to establish ten new arrangements and submitted a request for two others. CSIS also modified or expanded one foreign arrangement and asked for Ministerial approval to expand three others.

At the end of fiscal year 2004–2005, the Service had 257 foreign arrangements with 143 countries.

Of the Service's 257 foreign arrangements, 42 were identified as dormant (with dormancy defined as no liaison contact for at least one year). The Service continues to maintain restrictions on exchanges of information in the case of five of these dormant arrangements, due to:

- concerns about the foreign agency's human rights record;
- one or more violations of the rule against transferring information to a third party; or
- an overall lack of reliability of the liaison contact.

The Service can opt to re-activate dormant arrangements in cases where regional conflicts and political events that may affect Canadian national security interests may transpire.

The FLV Branch is also responsible for security liaison posts. As part of its foreign liaison program, the Service maintains security liaison posts abroad, normally co-located with Canadian diplomatic missions. The Service relies heavily on its security liaison posts to assess the usefulness of individual CSIS Section 17 foreign arrangements, as well as the reliability of those foreign agencies. These posts also provide significant

support to Citizenship and Immigration Canada related to Sections 14 and 15 immigration screening requirements (*see Report # 2004-01 in this year's annual report*).

The FLV also coordinates visits to CSIS Headquarters and CSIS Regional Offices by foreign agency representatives, including foreign ambassadors, as well as travel abroad by Service representatives.

CSIS DOMESTIC ARRANGEMENTS

The discharge of the Service's mandate under Sections 12–16 of the *CSIS Act* routinely requires cooperation among governments at the federal and provincial level, as well as with police services in a given province. Cooperation can take the form of exchanges of information, providing operational assistance, or conducting joint operations. CSIS does not require a formal arrangement when disclosing information to any domestic government department, agency or police service in accordance with its responsibility to advise government. Classified information passed under these circumstances to any federal department or agency is protected under normal provisions of the Government Security Policy.

CSIS entered into an arrangement with the Prime Minister's National Security Advisor in the Privy Council Office with respect to the establishment and management of the Integrated Threat Assessment Centre.

However, under Section 17(1)(a) of the *CSIS Act*, the Service may, with the approval of the Minister, conclude written cooperation arrangements—referred to as memoranda of understanding—with domestic agencies for the purpose of performing its duties and functions.

In the year under review, CSIS entered into an arrangement with the Prime Minister's National Security Advisor in the Privy Council Office with respect to the establishment and management of the Integrated Threat Assessment Centre, making a total of 17 such arrangements with federal institutions. The number of domestic arrangements with the provinces (10) remained unchanged. There were no terminations or amendments to existing arrangements.

Relationship with the RCMP

Among domestic arrangements, the Memorandum of Understanding between CSIS and the RCMP figures most prominently in SIRC's review because of the volume of exchanges between these two organizations and their ongoing history of joint operations.

In 2004–2005, there were 855 written or verbal exchanges of information provided to the Service by the RCMP—a significant increase over the 615 exchanges in the previous year. The Service, for its part, provided the RCMP with 227 disclosure letters in 2004–2005, and 215 in the previous year. A disclosure letter from CSIS is required to allow the RCMP to use Service information to pursue a criminal investigation.

During 2004–2005, CSIS also provided the RCMP with 24 advisory letters—compared to 15 letters in 2003–2004. The RCMP request advisory letters from the Service to use CSIS information in court proceedings.

In 2004–2005, there were 855 written or verbal exchanges of information provided to the Service by the RCMP—a significant increase over the 615 exchanges in the previous year.

The year under review marks the fourth year of operation for the RCMP-led Integrated National Security Enforcement Teams (INSETs), to which CSIS staff from four regions, as well as CSIS Headquarters, have been seconded. The Service reports that the INSETs have proven to be beneficial in that they have fostered closer cooperation between the Service and the RCMP. Because INSETs are operationally led by the RCMP, SIRC has a very limited capacity to review their activities—and indeed these joint operations once again highlight the limitations of SIRC's mandate in the increasingly operationally integrated security sector.

This year, two SIRC studies (2004-02 and 2004-07) examined the substance of the information exchanged with the RCMP and the nature of cooperation between the two organizations during the course of its reviews of regional offices and CSIS investigations.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available to the Government of Canada. They provide an organization with Federal Court authorization to use investigative techniques—such as monitoring of telephone communications—that would otherwise be illegal. For this reason alone, the use of warrants by CSIS deserves continued scrutiny—a task that SIRC takes very seriously. In the course of the Committee's in-depth reviews of CSIS investigations, the individual warrants (along with their supporting documentation), are generally the subject of detailed examination.

Table 6
New and Replaced/Renewed/Supplementary Warrants

	2002–2003	2003–2004	2004–2005
New warrants	52	68	40
Replaced/Renewed/Supplementary	150	130	207
Total	**202**	**198**	**247**[17]

Every year, SIRC asks CSIS to provide statistics on the Service's request for warrants (i.e., the information CSIS provides the Court in seeking a warrant), as well as on warrants granted by the Federal Court. Table 6 compares the number of warrants issued in each of the last three fiscal years.

In 2004–2005 most warrants were approved for one year. A select few were approved for a shorter span at the request of the Service. This was done to allow the expiration of these warrants to coincide with the expiration dates of other warrants on related files.

For three applications, the Court asked the Service for interim reports to provide the Court with up-to-date information on the status of a target, or to justify the continued need for—or usefulness of—the warrants.

In another case, the Court declined to grant one of the powers sought by the Service until the Court had been provided with more compelling evidence of the need for that power.

On several occasions, revisions were made to affidavits in support of applications during the hearings before the Federal Court. In one instance, the Court adjourned the hearing so that the Service could make changes. The application was approved after the submission of amended documents.

> The use of warrants by CSIS deserves continued scrutiny—a task that SIRC takes very seriously.

The Federal Court did not impose any new conditions or revise any existing conditions on warrants during the fiscal year under review. The Service also reported that in 2004–2005, no judicial decisions affected its applications for warrants, the execution of powers contained in warrants, or the warrant process in general.

17. The increase in warrant totals reflects a revised process for calculating statistics and does not represent an increase in the Service's targeting.

According to the Service, the Federal Court issued nine urgent warrants during 2004–2005, compared to 30 in the previous year.

Also of note, Section 28 of the *CSIS Act* authorizes the Governor-in-Council to make regulations governing: the forms of warrants; the practice and procedure applicable to the hearing of applications; as well as the place where (and the manner in which) hearings may be held. There were no regulations made in 2004–2005.

Section 3

Want to Know More?
An Overview of SIRC

Want to Know More? An Overview of SIRC

COMMITTEE MEMBERSHIP

During the 2004–2005 fiscal year, SIRC was chaired by the Honourable Paule Gauthier, P.C., O.C., O.Q., Q.C., who was first appointed Chair on September 30, 1996, and re-appointed to a second five-year term in 2000. M[me] Gauthier's appointment as Chair ended on June 7, 2005. On June 24, 2005, the Honourable Gary Filmon, P.C., O.M., was appointed as SIRC's new Chair, and M[me] Aldéa Landry, P.C., Q.C. was appointed as the Committee's newest member. Other Members of the Committee are: the Honourable Raymond Speaker, P.C., O.C. (reappointed on September 16, 2004, to a new five-year term); the Honourable Baljit Chadha, P.C.; and the Honourable Roy Romanow, P.C., O.C., Q.C.

On June 24, 2005, the Honourable Gary Filmon, P.C., O.M., was appointed as SIRC's new Chair, and M[me] Aldéa Landry, P.C., Q.C. was appointed as the Committee's newest member.

All Members of the Committee are Privy Councillors, who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties. There were no vacancies on the Committee at the close of this fiscal year.

STAFFING AND ORGANIZATION

The Committee is supported by an Executive Director and a staff of 19, located in Ottawa. The staff comprises: an Associate Executive Director, a Deputy Executive Director, Senior Counsel, Counsel, Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), nine Researchers, a Corporate Services Manager and four administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

RESEARCH AND REVIEW ACTIVITIES

On an annual basis, the Committee identifies specific CSIS investigations and areas of responsibility for detailed review. Unforeseen events or new priorities may result in these reviews being supplemented by additional projects. SIRC analysts undertake the detailed research for each project, with direction from senior management and

regular reporting to the Committee. Given the highly classified and sensitive nature of the materials being reviewed, SIRC staff divide their time between SIRC's premises and a fully equipped office at CSIS Headquarters, set up for the exclusive use of Committee staff.

SECURITY INTELLIGENCE BRIEFINGS

As part of their ongoing information gathering, the Chair of SIRC, Committee Members, and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community. These exchanges are supplemented by discussions with academics, security and intelligence experts and relevant non-governmental organizations, such as human rights groups. Such activities enrich the Committee's knowledge about the range of issues and opinions affecting the security intelligence field. The Committee also visits CSIS regional offices on a rotating basis to examine how Ministerial Direction and CSIS policy affect the day-to-day work of investigators in the field. These trips give Committee Members an opportunity to meet with senior CSIS staff, to receive briefings on local issues, challenges, priorities and perspectives, and to communicate the Committee's focus and concerns. During the 2004–2005 fiscal year, the Committee visited two regional offices.

ADDITIONAL COMMITTEE ACTIVITIES

- On September 8, 2004, SIRC's Executive Director addressed the Interim Committee of Parliamentarians, which was established to consult and make recommendations regarding the proposed statutory Committee of Parliamentarians on National Security.

- The Chair, Committee Members, and Executive Director attended the International Intelligence Review Agencies Conference in Washington, D.C., October 3–5, 2004. The Committee stayed an extra day to meet with representatives from the oversight bodies of the American security and intelligence community.

- On October 6, 2004, the British High Commission visited SIRC's office to introduce the new Chief of the British Security Intelligence Services, who was appointed in August 2004.

- On October 6, 2004, the Associate Executive Director, on behalf of the Executive Director, was a guest lecturer at a Carleton University Canadian Centre of Intelligence and Security Studies seminar on intelligence, statecraft and international affairs. The Associate Executive Director provided students with an overview of SIRC.

- The Executive Director attended the Canadian Centre of Intelligence and Security Studies (CCISS) Conference in Ottawa on April 14–15, 2004, entitled "Conference on the Gouzenko Affair: The Beginnings of Canadian Counter-Espionage and Cold

War Intelligence History." The Executive Director is a member of the board of advisors for the CCISS.

- The Executive Director and several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa on October 14–17, 2004.

- On November 26, 2004, the Executive Director and Deputy Executive Director met with members of the Netherlands Supervisory Committee on the Intelligence and Security Services.

- On March 21, 2005, the Executive Director gave a presentation to the students of the "National Security and Intelligence in the Modern State" course at Carleton University.

- In Spring 2005, SIRC released *Reflections*—a publication that recounted the watershed events over the Committee's 20-year history, including the McDonald Commission, the passage of the *CSIS Act*, as well as key reviews and complaint cases that SIRC has undertaken over the past two decades. It also provided detailed information on the inner workings of the Committee—helping to raise public awareness about SIRC's role and responsibilities.

BUDGET AND EXPENDITURES

The Committee continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. In December 2004, Parliament approved Supplementary Estimates, which increased SIRC's budget by $344,000 in 2004–2005, as well as in future years. This was based on a 2002 Treasury Board submission in which SIRC presented a business case explaining why additional funding was required to keep abreast of a 30% increase in CSIS's budget. This new funding was used mainly to hire additional research staff. Table 7 below presents a breakdown of actual and estimated expenditures.

Table 7
SIRC Expenditures

	2004–2005 (Actual $)	2005–2006 ($ Estimates)
Personnel	1,766,330	1,777,000
Operating	886,822	1,019,000
Total	**2,653,152**	**2,796,000**

INQUIRIES UNDER THE ACCESS TO INFORMATION AND PRIVACY ACTS

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 8, *Requests for Release of Information*, outlines the number of requests SIRC has received under these acts for the past three fiscal years.

Access to Information requests for the Committee's studies represent the largest portion of the access requests. The work required to prepare a report for public release need only be done once, but this benefits all subsequent requesters. Consequently, the Committee waives the application fees for all requests for access to its studies.

Table 8
Requests for Release of Information

Year	*Access to Information Act*	*Privacy Act*
2002–2003	20	4
2003–2004	31	1
2004–2005	21	3

MODERN COMPTROLLERSHIP

SIRC made significant progress on the implementation of modern comptrollership initiatives during this fiscal year. The organization completed a management action plan, a risk assessment, an audit plan and developed performance indicators. Additional work in support of the implementation of modern comptrollership will continue in the new fiscal year. Given its small staff complement and the absence of dedicated, functional specialists, SIRC often relies on contracted resources to obtain the necessary expertise for this initiative.

Appendix A

Acronyms

Acronyms

CBSA	Canada Border Services Agency
CCRA	Canada Customs and Revenue Agency
CHRA	*Canadian Human Rights Act*
CI	Counter Intelligence
CIB	CSIS Intelligence Brief
CIC	Citizenship and Immigration Canada
CP	Counter Proliferation
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism
DND	Department of National Defence
EDE	Electronic Data Exchange
FAC	Foreign Affairs Canada
FES	Front-End Screening
FLV	Foreign Liaison and Visits
HQ	CSIS Headquarters, Ottawa
IG	Inspector General
INSAC	Integrated National Security Assessment Centre
INSETS	Integrated National Security Enforcement Teams

IOC	Information Operations Centre
IRPA	*Immigration and Refugee Protection Act*
ITAC	Integrated Threat Assessment Centre
LAP	Liaison Awareness Program
OSFI	Office of the Superintendent of Financial Institutions
PSEP	Public Safety and Emergency Preparedness
RAP	Research, Analysis and Production
RCMP	Royal Canadian Mounted Police
RTA	Request for Targeting Authority
SIR	Security Intelligence Report
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer
TAU	Threat Assessment Unit
TCA	Transnational criminal activity
TEL	Terrorist Entity Listing
TFA	Terrorist Financing Unit
UNAR	*United Nations Afghanistan Regulations*
UNSTR	*United Nations Suppression of Terrorism Regulations*
WMD	Weapons of Mass Destruction

Appendix B

SIRC Reports and Studies Since 1984

SIRC Reports and Studies Since 1984

(Section 54 reports—special reports the Committee makes to the Minister—are indicated with an *)

1. *Eighteen Months After Separation: An Assessment of CSIS Approach to Staffing Training and Related Issues* (SECRET) * (86/87-01)

2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service* (SECRET) * (86/87-02)

3. *The Security and Intelligence Network in the Government of Canada: A Description* (SECRET) * (86/87-03)

4. *Ottawa Airport Security Alert* (SECRET) * (86/87-05)

5. *Report to the Solicitor General of Canada Concerning CSIS Performance of its Functions* (SECRET) * (87/88-01)

6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS* (UNCLASSIFIED)* (86/87-04)

7. *Counter-Subversion: SIRC Staff Report* (SECRET) (87/88-02)

8. *SIRC Report on Immigration Screening* (SECRET) * (87/88-03)

9. *Report to the Solicitor General of Canada on CSIS Use of Its Investigative Powers with Respect to the Labour Movement* (PUBLIC VERSION) * (87/88-04)

10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process* (SECRET)* (88/89-01)

11. *SIRC Review of the Counter-Terrorism Program in the CSIS* (TOP SECRET) * (88/89-02)

12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS* (SECRET) * (89/90-02)

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (SECRET) * (89/90-03)

14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information* (SECRET) (89/90-04)

15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information* (SECRET) * (89/90-05)

16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons* (UNCLASSIFIED) (89/90-06)

17. *SIRC Report on the Innu Interview and the Native Extremism Investigation* (SECRET) * (89/90-07)

18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988* (SECRET) * (89/90-01)

19. *A Review of the Counter-Intelligence Program in the CSIS* (TOP SECRET) * (89/90-08)

20. *Domestic Exchanges of Information* (SECRET) * (90/91-03)

21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue* (SECRET) (90/91-06)

22. *Regional Studies* (six studies relating to one region) (TOP SECRET) (90/91-04)

23. *Study of CSIS Policy Branch* (CONFIDENTIAL) (90/91-09)

24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets* (TOP SECRET) (90/91-05)

25. *Release of Information to Foreign Agencies* (TOP SECRET) * (90/91-02)

26. *CSIS Activities Regarding Native Canadians—A SIRC Review* (SECRET) * (90/91-07)

27. *Security Investigations on University Campuses* (TOP SECRET) * (90/91-01)

28. *Report on Multiple Targeting* (SECRET) (90/91-08)

29. *Review of the Investigation of Bull, Space Research Corporation and Iraq* (SECRET) (91/92-01)

30. *Report on Al Mashat's Immigration to Canada* (SECRET) * (91/92-02)

31. *East Bloc Investigations* (TOP SECRET) (91/92-08)

32. *Review of CSIS Activities Regarding Sensitive Institutions* (TOP SECRET) (91/92-10)

33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)

34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) * (91/92-04)

35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)

36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)

37. *Threat Assessments, Section 40 Study* (SECRET) * (91/92-07)

38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) * (92/93-01)

39. *"STUDYNT" The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)

40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) * (90/91-13)

41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)

42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)

43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)

44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) * (90/91-10)

45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review* (TOP SECRET) * (91/92-14)

46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)* (TOP SECRET) * (90/91-11)

47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)

48. *Domestic Exchanges of Information (A SIRC Review—1991/92)* (SECRET) (91/92-16)

49. *Prairie Region Audit* (TOP SECRET) (90/91-11)

50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)

51. *Regional Audit* (TOP SECRET)

52. *A SIRC Review of CSIS SLO Posts (London & Paris)* (SECRET) (91/92-11)

53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)

54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93-03)

55. *Domestic Investigations (1)* (SECRET) (CT 93-02)

56. *Domestic Investigations (2)* (TOP SECRET) (CT 93-04)

57. *Middle East Movements* (SECRET) (CT 93-01)

58. *A Review of CSIS SLO Posts (1992-93)* (SECRET) (CT 93-05)

59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93-01)

60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)

61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)

62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)

63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93-11)

64. *Sources in Government* (TOP SECRET) (CI 93-09)

65. *Regional Audit* (TOP SECRET) (CI 93-02)

66. *The Proliferation Threat* (SECRET) (CT 93-07)

67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) * (CT 94-02)

68. *A Review of CSIS' SLO Posts (1993–94)* (SECRET) (CT 93-09)

69. *Domestic Exchanges of Information (A SIRC Review 1993–94)* (SECRET) (CI 93-08)

70. *The Proliferation Threat — Case Examination* (SECRET) (CT 94-04)

71. *Community Interviews* (SECRET) (CT 93-11)

72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) * (CI 93-07)

73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)

74. *A SIRC Review of CSIS SLO Posts (1994–95)* (SECRET) (CT 95-01)

75. *Regional Audit* (TOP SECRET) (CI 93-10)

76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)

77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)

78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)

79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)

80. *Domestic Exchanges of Information (A SIRC Review 1994–95)* (SECRET) (CI 94-03)

81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)

82. *CSIS and a "Walk-In"* (TOP SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)

84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)

85. *Regional Audit* (TOP SECRET) (CT 95-02)

86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95-03)

87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)

88. *Homeland Conflict* (TOP SECRET) (CT 96-01)

89. *Regional Audit* (TOP SECRET) (CI 96-01)

90. *The Management of Human Sources* (TOP SECRET) (CI 96-03)

91. *Economic Espionage I* (SECRET) (CI 96-02)

92. *Economic Espionage II* (TOP SECRET) (CI 96-02)

93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96-04)

94. *Urban Political Violence* (SECRET) (SIRC 1997-01)

95. *Domestic Exchanges of Information (1996–97)* (SECRET) (SIRC 1997-02)

96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997-03)

97. *Regional Audit* (TOP SECRET) (SIRC 1997-04)

98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997-05)

99. *Spy Case* (TOP SECRET) (SIRC 1998-02)

100. *Domestic Investigations (3)* (TOP SECRET) (SIRC 1998-03)

101. *CSIS Cooperation with the RCMP—Part I* (SECRET) * (SIRC 1998-04)

102. *Source Review* (TOP SECRET) (SIRC 1998-05)

103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998-06)

104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998-08)

105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)

106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)

107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)

108. *CSIS Cooperation with the RCMP—Part II* (SECRET) * (SIRC 1998-04)

109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98* (TOP SECRET) (SIRC 1998-07)

110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)

111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)

112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)

113. *Allegations by a Former CSIS Employee* (TOP SECRET) * (SIRC 1998-12)

114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)

115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC 1998-15)

116. *Files* (TOP SECRET) (SIRC 1998-16)

117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET) (SIRC 1999-01)

118. *A Long-Running Counter-Intelligence Investigation* (TOP SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)

120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) * (SIRC 1999-05)

122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)

124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)

125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)

126. *Project Sidewinder* (TOP SECRET) * (SIRC 1999-10)

127. *Security Breach* (TOP SECRET) (SIRC 1999-11)

128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)

129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)

130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)

131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)

132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)

133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)

134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET) (SIRC 2002-01)

135. *Source Recruitment* (TOP SECRET) (SIRC 2001-01)

136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001-05)

137. *Domestic Extremism* (TOP SECRET) (SIRC 2001-03)

138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET) (SIRC 2001-04)

139. *Warrant Review* (TOP SECRET) (SIRC 2001-06)

140. *Special Report following allegations pertaining to an individual* (TOP SECRET) *

141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)

142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)

143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)

144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)

145. *Special Report (2002-2003) following allegations pertaining to an individual* (TOP SECRET) *

146. *Front End Screening Program* (TOP SECRET) (SIRC 2003-01)

147. *CSIS Section 12 Operational Activity Outside Canada* (TOP SECRET) (SIRC 2003-02)

148. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2003-03)

149. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2003-04)

150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2003-05)

151. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2004-01)

152. *Review of CSIS's Investigation of Transnational Criminal Activity* (TOP SECRET) (SIRC 2004-02)

153. *Review of the Terrorist Entity Listing Process* (SECRET) (SIRC 2004-03)

154. *Review of Activities and Investigations in a CSIS Regional Office* (TOP SECRET) (SIRC 2004-04)

155. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2004-05)

156. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2004-06)

157. *Review of CSIS's Information Operations Centre* (TOP SECRET) (SIRC 2004-07)

158. *Review of CSIS's Exchanges of Information with Close Allies* (TOP SECRET) (SIRC 2004-08)

159. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2004-09)

160. *Terrorist Financing Activities in Canada* (TOP SECRET) (SIRC 2004-10)

161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TOP SECRET) *

Appendix C

Key Findings and Recommendations

Key Findings and Recommendations

REVIEW OF THE TERRORIST ENTITY LISTING PROCESS

In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*, specifically the Service's role in the Terrorist Entity Listing (TEL) process. The TEL process is mandated under Section 83.05 of the *Criminal Code*, as amended by the *Anti-Terrorism Act*. CSIS's role in the TEL process is the creation of Security Intelligence Reports (or SIRs), considered by the Minister of Public Safety and Emergency Preparedness in her recommendation to the Governor-in-Council concerning whether or not an entity should be listed.

The Committee contends that the listing process may require CSIS to collect, retain, and analyze information that does not fall within the definition of "threats to the security of Canada" as defined in the *CSIS Act*. Overall, in the Committee's review of the Service's role in the TEL process, SIRC found that the Service's collection of information for the listing process was undertaken in accordance with Ministerial Direction—once this direction was provided—and according to relevant operational policies. Nevertheless, SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to "threats to the security of Canada."

The Committee was unable to have access to the SIRs during its review of the Service's role in the TEL process, owing to Cabinet confidence. While SIRC was able to perform a reasonably comprehensive review of CSIS's role in this process, its efforts nevertheless fell short of a complete assessment.

REVIEW OF CSIS'S INVESTIGATION OF TRANSNATIONAL CRIMINAL ACTIVITY

This review assessed CSIS's investigation of transnational criminal activities (TCA) and focussed on the Canadian-based activities of several foreign-based, transnational organized crime groups. The investigations sampled for this review were national in scope and subject to Level II and Level III targeting investigations into suspected threat-related activities as described in Section 2(b) of the *CSIS Act*.

SIRC concluded that CSIS had reason to believe that the activities of the four individual targets were foreign-directed or undertaken on behalf of foreign interests, and generally represented a threat as defined in Section 2(b) of the *CSIS Act*. In addition, SIRC

found that the Service complied fully with Ministerial Direction and operational policy in applying for targeting authorization. It also applied a level of intrusiveness proportionate to the suspected threats.

There were no recommendations arising from this review.

REVIEW OF A COUNTER-TERRORISM INVESTIGATION

This study outlined the results of SIRC's examination of a CSIS counter-terrorism investigation that had not been the focus of a comprehensive SIRC review in over a decade, yet has remained a high priority of the Counter Terrorism Branch. This investigation was the subject of a Level III targeting authority for suspected threat-related activities as described in Section 2(c) of the *CSIS Act*.

The Committee selected for in-depth review one issue-based target, one targeted organization, six individual targets, one warrant and six human-source operations. SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining key operational activities. SIRC found that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat.

There were no recommendations arising from this study.

REVIEW OF ACTIVITIES AND INVESTIGATIONS IN A CSIS REGIONAL OFFICE

SIRC endeavours each year to undertake a comprehensive review of CSIS's activities in a particular region. This type of review looks at the targeting of individuals, implementation of warrant powers, use of human sources, as well as cooperation and exchanges of information with Canadian and foreign partners. SIRC also reviewed CSIS's internal security measures for the region, as well as any security violations and breaches between April 1, 2000–March 31, 2003.

Overall, the region's investigative activities during the review period complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC found that CSIS had reasonable grounds to suspect the authorized targets of investigation posed a threat to the security of Canada, and that the intrusiveness of the techniques used were proportionate to the suspected threat these targets posed.

During the review, SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. Based on this, the Committee

found that the organization had a dual function. SIRC believes operational policy governing investigations that have an impact on, or appear to have an impact on one function should apply to this organization. CSIS disagreed with this finding.

The Committee recommended that CSIS define a term in its operational policy.

REVIEW OF A COUNTER-PROLIFERATION INVESTIGATION

This study examined the Service's investigation of the threat to Canadian security posed by activities related to the proliferation of weapons of mass destruction by persons or organizations linked to a certain country.

SIRC found that the Service complied fully with Ministerial Direction and operational policy with respect to applications for targeting authorization and approvals for each of the investigations reviewed by SIRC. The Committee concluded that the Service had reasonable grounds to suspect that each of the authorized targets of investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation was proportionate to the suspected threat. CSIS collected only information strictly necessary to fulfill its mandate.

SIRC endorsed the Service's approach of engaging relevant private-sector entities, undertaken via the Liaison Awareness Program (LAP). The Service met all of the requirements of the *CSIS Act* and operational policy with respect to warrant acquisition. SIRC concluded that one CSIS regional office did not comply fully with policy requirements concerning the timely provision of verbal and written tasking to the employee responsible for monitoring intercepted communications. CSIS adhered to policy requirements and Ministerial Direction in the management of the human-source operations reviewed. Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy.

There were no recommendations arising from this review.

REVIEW OF CSIS'S INFORMATION OPERATIONS CENTRE

SIRC undertook its first-ever review of CSIS's investigation of threats against Canada's critical information infrastructure. It did so with two objectives. First, SIRC reviewed the role of the Information Operations Centre (IOC) in investigating threats against Canada's critical information infrastructure. Second, the Committee reviewed the IOC's operations, examining one counter-intelligence investigation of an information operation for compliance with the *CSIS Act*, Ministerial Direction and Service operational policies.

Notwithstanding two concerns identified below, SIRC found that in carrying out its duties and functions, the Service complied with the *CSIS Act*, Ministerial Direction and CSIS operational policies. SIRC's first concern was that operational policy keep pace with the matter reviewed.

> **SIRC recommends that the Service review operational policy to ensure that it clearly incorporates certain matters in relation to Section 12 targeting.**

The Committee's second concern was related to administrative errors.

> **SIRC recommends that the Service review operational policy to ensure that if it is necessary to cross-reference operational database reports recorded under one file number with reports recorded under another file number, this should be noted in the "Investigator's Comments" section of the reports.**

REVIEW OF CSIS'S EXCHANGES OF INFORMATION WITH CLOSE ALLIES

The case of Mr. Arar focussed public attention on the use of information that may have been collected in Canada and then shared with Canada's foreign partners. The Committee decided to undertake its first in-depth examination of CSIS's exchanges of information with close allied partners. Drawing on one of the Service's counter-terrorism investigations, SIRC chose to review CSIS's information exchanges with four allied agencies as the focus of the detailed review.

In the context of the investigation that was reviewed, SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy. The Committee also found that the Service exercised due diligence in exchanging information about targets of investigation.

While the Service obtained appropriate approval prior to disclosing information to selected allied agencies, SIRC found that operational policy should accurately reflect which managerial level is accountable for information exchanged with foreign agencies.

> **SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies.**

In this study, SIRC also examined how human rights were addressed within the context of foreign arrangements. When CSIS initiates the process to enter into a new arrangement with a foreign agency, it informs Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness that it will "closely scrutinize the content of the information provided to, or received from, a foreign agency in order to ensure that none of the information sent to, or received from, that agency is used in the commission of, or was obtained as a result of, acts that could be regarded as human rights violations." However, the Committee concluded that CSIS was not in a position to provide such an absolute assurance.

SIRC recommended that CSIS revise the content of the letters to Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness to avoid leaving any impression that it can guarantee that information sent to, or received from, a foreign agency was not used in the commission of, nor was obtained as a result of, acts that could be regarded as human rights violations.

REVIEW OF A COUNTER-INTELLIGENCE INVESTIGATION

SIRC examined this counter-intelligence investigation for the period January 1, 2003, to December 31, 2003. The objective was to assess the Service's compliance with the *CSIS Act*, Ministerial Direction and all relevant operational policies.

Overall, the counter-intelligence investigation was in compliance with the *CSIS Act*, Ministerial Direction and operational policy during the review period. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada. Moreover, the Committee found that the intrusiveness of the techniques used were proportionate to the suspected threat that these targets posed. CSIS investigators only collected information that was strictly necessary for the investigation. They also acted appropriately and within the law in their use of human sources.

Throughout the review, SIRC paid particular attention to CSIS's investigation of interference activities. SIRC found that CSIS's operational policies covering these types of situations were incomplete. Because of this, the Committee recommended that:

CSIS review and amend, where appropriate, its operational policies relating to specific institutions to ensure that they cover all aspects of a given process.

TERRORIST FINANCING ACTIVITIES IN CANADA

The objective of this study was to examine CSIS's investigation of terrorist financing activities in Canada for in-depth review. SIRC selected one issue-based target, and five specific targets. In each case, the Committee assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy.

The Committee concluded that the Service had reasonable grounds to suspect that the activities of targeted individuals and groups posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat, and CSIS collected only that information necessary to fulfill its mandate. The Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC was satisfied with the degree and nature of the Service's cooperation with domestic and foreign partners.

It is possible that the Service may be required to collect and analyze information regarding an entity that meets the definition of a *listed person or group* under the *United Nations Suppression of Terrorism Regulations* (UNSTR), but does not represent a *threat to the security of Canada* under Section 12 of the *CSIS Act*. Further, SIRC noted that the UNSTR does not specifically direct the Service to participate in the listing process, nor has the Minister of Public Safety and Emergency Preparedness provided CSIS with specific direction to that effect.

There were no recommendations arising from this study.

CSIS LIAISON WITH FOREIGN AGENCIES: REVIEW OF A SECURITY LIAISON POST

SIRC sought to determine whether exchanges of information from this post with foreign agencies were within the scope of the government-approved liaison agreements in place. The Committee also assessed the operations at the security liaison post in relation to the *CSIS Act*, Ministerial Direction, and the Service's operational policies and procedures.

For context, SIRC also reviewed this post's operations, and evaluated them against issues raised in SIRC's ongoing statutory reviews of CSIS's Foreign Arrangements. Moreover, the report considered trends identified in SIRC's SLO studies over the previous five years.

SIRC was concerned by the lack of updated CSIS documents to assess the liaison relationships at the post. While there are written guidelines for the creation, submission and updating of these documents, there are no formal CSIS policies governing this activity. The Committee made the following recommendation:

> **The Committee recommended that the Service create policies for the preparation, updating and annual submission of CSIS documents used to assess the scope of exchanges with foreign agencies.**

REVIEW OF FOREIGN ARRANGEMENTS

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with the government of a foreign state, or an international organization of states (or an institution thereof), for the purpose of performing its duties and functions. Section 38(a)(iii) of the *CSIS Act* directs SIRC to review all such arrangements. During 2004–2005, SIRC undertook its first comprehensive review of the expansion process. An enhancement or expansion occurs when the Service changes an existing arrangement. This defines the subject matter and extent of authorized exchanges.

SIRC found that CSIS complied with the conditions set out in Ministerial Direction and operational policy regarding the expansion of the ten existing foreign arrangements. With respect to expansion approvals, SIRC noted that the Service has no operational policy on what type of information must be contained in the request submitted to the Director. The Committee also noted that the assessment of agencies with whom the Service has arrangements were not always submitted on a yearly basis as required in the Foreign Liaison Post Procedures Manual.

There were no recommendations arising from this review.

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Rapport annuel du CSARS 2004-2005

Examen opérationnel du Service canadien du renseignement de sécurité

Canada

Comité de surveillance des activités de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario)
K1P 5W5

Téléphone : (613) 990-8441
Télécopieur : (613) 990-5230
Site Web : http://www.sirc-csars.gc.ca
Les appels à frais virés sont acceptés de 8 h à 17 h, heure normale de l'Est.

Nota : Aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Travaux publics et Services gouvernementaux Canada 2005
N° de cat. PS105-2005
ISBN 0-662-69304-3

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Rapport annuel du CSARS 2004-2005

Examen opérationnel du Service canadien du renseignement de sécurité

Canada

Le 30 septembre 2005

L'honorable Anne McLellan, C.P., députée
Vice-première ministre et ministre de la Sécurité publique et de la Protection civile
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Madame la Ministre,

Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous présentons au Parlement, par votre entremise, le rapport du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2004-2005.

Veuillez agréer, Madame la Ministre, l'expression de notre haute considération.

Le président,

Gary Filmon, C.P., O.M.

Baljit S. Chadha, C.P.

Roy Romanow, C.P., O.C., c.r.

Raymond Speaker, C.P., O.C.

M^me^ Aldéa Landry, C.P., c.r.

Table des matières

Déclaration du Comité ix

Au sujet du présent rapport xi
Agencement du rapport xi
Sélection des études à mener par le CSARS : choix et défis xii

Section 1 : bilan de 2004-2005 1

A. Études des activités de renseignement de sécurité du SCRS ... 3
Aperçu des modalités de la fonction de surveillance du CSARS 3
Rôle du Comité au sein de la structure redditionnelle du SCRS 3
Études du CSARS en 2004-2005 4
Examen du processus d'inscription des entités terroristes 4
Étude de l'enquête du SCRS sur la criminalité transnationale 11
Étude d'une enquête antiterroriste 15
Examen des activités et enquêtes d'un bureau régional du SCRS 18
Étude d'une enquête en matière de lutte contre la prolifération 21
Examen du Centre des opérations d'information du SCRS 23
Examen des échanges d'information du SCRS avec les proches alliés .. 25
Étude d'une enquête de contre-espionnage 28
Financement du terrorisme au Canada 30
Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité 33
Examen des ententes avec des organismes étrangers 36

B. Enquêtes sur les plaintes 39
Rapports de décisions : résumés des plaintes 40
Rapport : renvoi d'une plainte en matière de droits de la personne . 40
Rapport : article 41 (« activités du Service ») 41
Rapport : article 42 (refus d'une habilitation de sécurité) 42

C. Rapport au ministre de la Sécurité publique et de la Protection civile selon l'article 54 44

Section 2 : mécanismes redditionnels du SCRS 47

A. Exigences en matière de rapports 49
Certificat de l'inspecteur général pour 2004 49
Rapport opérationnel annuel du directeur du SCRS, 2003-2004 50
Agissements illicites de la part du SCRS 53
Enquêtes en vertu de l'alinéa 2*d)* 53
Communication d'informations pour raisons d'intérêt public ou national 54

B. Cadre d'action et de gestion 55
Exigences nationales annuelles en matière de renseignement de sécurité 55
Instructions du Ministre 57
Règlements et nominations par le gouverneur en conseil 57
Modifications à la politique opérationnelle du SCRS 58

C. Activités du SCRS sur le plan opérationnel 59
Lutte contre la prolifération 59
Antiterrorisme 60
Contre-espionnage 61
Direction de la recherche, de l'analyse et de la production 61
Filtrage de sécurité 62
Ententes du SCRS avec des organismes canadiens 72
Mandats de la Cour fédérale : généralités et statistiques 73

Section 3 : vous souhaitez en savoir plus? Coup d'œil sur le CSARS 77
Composition du Comité 79
Personnel et organisation 79
Activités de recherche et de surveillance 80
Exposés sur le renseignement de sécurité 80
Autres activités du Comité 80
Budget et dépenses 82
Demandes en vertu des *Lois sur l'accès à l'information* et *sur la protection des renseignements personnels* 82
La fonction de contrôleur moderne 83

Annexe A : sigles employés dans le rapport 85

Annexe B : rapports et études du CSARS depuis 1984 89

Annexe C : principales constatations et recommandations 101

Examen du processus d'inscription des entités terroristes 103
Étude de l'enquête du SCRS sur la criminalité transnationale 103
Étude d'une enquête antiterroriste 104
Examen des activités et enquêtes d'un bureau régional du SCRS 104
Étude d'une enquête en matière de lutte contre la prolifération 105
Examen du Centre des opérations d'information du SCRS 106
Examen des échanges d'information du SCRS avec les proches alliés 106
Étude d'une enquête de contre-espionnage 107
Financement du terrorisme au Canada 108
Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité 109
Examen des ententes avec des organismes étrangers 109

Déclaration du Comité

Le renseignement de sécurité au Canada face à de nouveaux défis vingt ans après l'établissement de la *Loi sur le SCRS*

Il y a maintenant vingt ans que voyaient le jour le Comité de surveillance des activités de renseignement de sécurité (CSARS) et le Service canadien du renseignement de sécurité (SCRS). Devant l'ensemble de ces deux décennies, c'est peu dire que le domaine de la sécurité nationale et mondiale a beaucoup changé. Et pourtant, un point sur lequel on ne saurait trop insister est la proportion de ces changements qui sont survenus depuis cinq ans. Au Canada et dans le monde entier, de nombreux services de renseignement de sécurité ont dû réorienter rapidement leur action, axée principalement sur le contre-espionnage, vers la lutte au terrorisme sur le plan national et international.

Le rythme de cette évolution s'est accéléré en 2001, au lendemain des attentats terroristes du 11 septembre, au fil des nouvelles mesures que la *Loi antiterroriste* a values aux Canadiens. Aujourd'hui, les activités de collecte d'information et d'évaluation sont réparties entre divers organismes fédéraux, de sorte que le contexte du renseignement de sécurité est à la fois plus complexe et plus intégré. Cela comporte d'importantes ramifications pour les citoyens et les décideurs : après tout, la raison d'être du CSARS était de faire contrepoids aux puissants pouvoirs intrusifs que la *Loi sur le SCRS* conférait au Service. Des pouvoirs semblables sont maintenant exercés par d'autres organes publics, dont certains n'ont pas le même regard scrutateur que celui du CSARS à l'endroit du SCRS.

Le CSARS applaudit à l'engagement du gouvernement à effectuer une intégration efficace de son appareil de renseignement opérationnel. Il appuie en outre la prochaine étape logique, soit un examen exhaustif et plus intégré de cet appareil. Comme bon nombre de Canadiens, nous avons hâte de connaître les constatations du juge Dennis O'Connor dont l'examen stratégique doit lui permettre de formuler des recommandations à l'égard d'un mécanisme de surveillance des activités de la GRC sur le plan de la sécurité nationale.

En plus de soutenir les efforts du Canada dans sa lutte intérieure contre le terrorisme, la *Loi antiterroriste* comporte une importante dimension internationale, soit harmoniser les lois canadiennes régissant cette lutte avec celles de ses partenaires étrangers. C'est cette dimension qui a élargi le champ des efforts déployés par le SCRS en matière de collecte de renseignements et qui a éprouvé la capacité du CSARS à mener un examen complet des activités du Service.

En effet, pour la première fois depuis bien des années, le CSARS se trouve dans la fâcheuse position d'être incapable d'examiner à fond certaines activités du Service : celles dont il s'est vu attribuer la responsabilité en vertu du *Code criminel* modifié par la *Loi antiterroriste* (question qui est exposée en détail plus loin, à la page 4. Ces activités représentent une fraction relativement minime du travail du SCRS, mais elles risquent fort de porter préjudice à certaines personnes.

En clair, voilà une question qui n'est pas du ressort du SCRS. Néanmoins, le Comité estime qu'il est d'une importance capitale que toutes les activités du Service, y compris leur élargissement, fassent l'objet d'un examen indépendant. Après tout, la *Loi sur le SCRS* a été adoptée par le Parlement afin que les pouvoirs considérables du Service soient définis clairement et surveillés.

Il importe donc, à notre avis, que le Parlement veille à ce que les lois régissant la surveillance soutiennent le rythme des mesures législatives qui appuient la capacité de renseignement. Une telle vigilance aidera à éviter de créer un vide en matière de surveillance du renseignement de sécurité.

En effet, beaucoup de choses ont changé depuis 1984, mais le cadre qui définit les pouvoirs et l'autorité tant du Service que du Comité a su résister à l'épreuve du temps. Les vingt dernières années ont permis de voir le CSARS et le SCRS évoluer afin de relever les défis du renseignement de sécurité au Canada, tout en amassant un héritage d'engagement face aux droits et à la primauté du droit. Nous espérons continuer à jouer un rôle vital au sein de la collectivité canadienne du renseignement de sécurité dans l'avenir.

Au sujet du présent rapport

Agencement du rapport

La raison d'être du Comité de surveillance des activités de renseignement de sécurité est d'assurer au Parlement du Canada, et par son entremise aux Canadiens, que le Service respecte la loi, les politiques et les instructions ministérielles dans l'exercice de ses fonctions. Le CSARS a deux fonctions principales. La première consiste à mener des études approfondies sur les activités du SCRS pour vérifier si elles sont conformes à la *Loi sur le SCRS* et aux divers instruments stratégiques qui en découlent ainsi qu'aux instructions du ministre de la Sécurité publique et de la Protection civile. La seconde consiste à recevoir les plaintes que toute personne peut porter à l'égard des activités du Service et à faire enquête à ce sujet.

Le rapport annuel de 2004-2005 est agencé en fonction des principales constatations du Comité. Les renseignements supplémentaires qui, à son avis, pourraient intéresser le lecteur par leur caractère documentaire, historique ou technique figurent dans des encadrés ombrés. Ces intercalaires visent à exposer des faits et ne reflètent ni les opinions ni les conclusions du CSARS.

Par sa présentation générale, le présent rapport annuel, à l'instar des précédents, établit une distinction entre les constatations, les observations et les recommandations que le Comité tire de ses études approfondies et de ses enquêtes sur les plaintes d'une part, et d'autre part les renseignements plus généraux qu'il recueille pour informer ses membres et éclairer le lecteur au sujet du contexte plus vaste dans lequel baigne le travail du SCRS en matière de renseignement de sécurité.

Section 1 : bilan de 2004-2005

Cette section fournit au lecteur un résumé des onze grandes études que le CSARS a menées pendant la période visée par le présent rapport. De plus, elle l'informe des plaintes que le Comité a reçues. Enfin, elle contient le résumé d'un rapport spécial qui a été présenté à la ministre de la Sécurité publique et de la Protection civile conformément à l'article 54 de la *Loi sur le SCRS*.

Agencement du rapport *(suite)*

Section 2 : mécanismes redditionnels du SCRS

Cette section décrit le cadre des politiques et de la régie à l'intérieur duquel le SCRS exerce ses fonctions. Elle expose aussi dans ses grandes lignes l'information que le Service fournit au CSARS au sujet des enquêtes de ses directions et des changements à ses plans et priorités opérationnels.

Section 3 : vous souhaitez en savoir plus? Coup d'œil sur le CSARS

Cette section fournit des détails sur les activités du Comité en matière de collecte d'information, de rayonnement, de liaison et d'administration, y compris le budget annuel et les dépenses du CSARS.

Sélection des études à mener par le CSARS : choix et défis

Le programme de recherche du CSARS est conçu pour englober un vaste éventail de sujets. Lorsqu'il en arrête le choix, le Comité tient compte des éléments suivants :

- l'ampleur des enquêtes du Service;
- les activités particulières qui pourraient porter atteinte aux droits et libertés individuels, ainsi que les priorités et préoccupations du Parlement et de la population canadienne;
- le rapport classifié du directeur du SCRS au Ministre, exposant les activités d'ordre opérationnel;
- l'importance d'évaluer régulièrement chacune des directions opérationnelles du Service et ses bureaux régionaux.

Le Comité tient en outre compte de divers autres facteurs lorsqu'il approuve les secteurs particuliers à scruter :

- les obligations que lui confère la *Loi sur le SCRS*, selon les détails qu'on y trouve;
- les événements susceptibles de présenter une menace envers la sécurité du Canada;
- les problèmes ou préoccupations mentionnés dans de précédents rapports du Comité;
- les engagements du CSARS à réexaminer des questions particulières;
- les questions cernées dans l'exercice des fonctions du Comité relativement aux plaintes;
- les nouvelles orientations stratégiques ou initiatives annoncées par le SCRS ou par le gouvernement du Canada.

Cette approche permet au Comité de gérer le risque inhérent de ne pouvoir examiner qu'un faible pourcentage des activités du SCRS une année donnée. Cependant, le CSARS est toujours prêt à moduler ses activités prévues afin de pouvoir faire face aux événements inattendus. Une étude spéciale de ce genre a été menée durant la période visée par le présent rapport. Il convient en outre de noter que le Comité a pu élargir son programme de recherche de 2004-2005 grâce aux nouvelles ressources que lui a procurées un budget supplémentaire des dépenses.

Pour chacune de ses études, le Comité procède à un examen détaillé de documents du SCRS, à des entrevues de cadres et de gestionnaires supérieurs du Service ainsi qu'à une évaluation des actions de celui-ci par rapport aux lois, politiques et instructions ministérielles applicables.

Le CSARS n'a qu'une petite équipe de recherchistes, mais il s'emploie à examiner l'éventail le plus vaste possible des fonctions du SCRS. Sur un certain nombre d'années, les divers projets de recherche qu'il a réalisés ont fourni au Parlement et à la population canadienne une description et une évaluation exhaustives des activités d'ordre opérationnel du Service.

Section 1

Bilan de 2004-2005

Bilan de 2004-2005

A. Études des activités de renseignement de sécurité du SCRS

Aperçu des modalités de la fonction de surveillance du CSARS

RÔLE DU COMITÉ AU SEIN DE LA STRUCTURE REDDITIONNELLE DU SCRS

Le Comité de surveillance des activités de renseignement de sécurité est le seul organisme indépendant de l'extérieur à être habilité par la loi et à avoir l'expertise voulue pour examiner les activités du SCRS. Il a été créé en vertu de la *Loi sur le SCRS* (1984) afin d'assurer au Parlement du Canada et aux Canadiens que le Service respecte la loi, les politiques et les instructions ministérielles dans l'exercice de ses fonctions. Ce faisant, le CSARS s'emploie à veiller au respect des droits fondamentaux et des libertés des Canadiens.

Pour remplir son mandat, le Comité confie chaque année à son personnel divers projets d'études qui fournissent un examen rétrospectif et une évaluation d'enquêtes et de fonctions particulières du SCRS. Il a des pouvoirs quasi illimités pour ce qui est de scruter l'exercice des fonctions du Service. Exception faite des seuls renseignements confidentiels du Cabinet, le CSARS a le pouvoir absolu d'examiner toute information touchant les activités du SCRS, quel qu'en soit le niveau de classification.

Le rapport de chaque étude contient des constatations et des recommandations du Comité. Une fois terminé, il est présenté au directeur et à l'inspecteur général du SCRS.

En vertu de l'article 54 de la *Loi sur le SCRS*, le CSARS est en outre autorisé à présenter au ministre de la Sécurité publique et de la Protection civile des rapports spéciaux sur toute question que ses membres estiment revêtir une importance particulière.

Cette fonction de surveillance permet au Comité d'informer le Parlement et la population du Canada au sujet des activités du Service et d'évaluer la conformité de celles-ci avec les lois du Canada, les instructions du Ministre et la politique opérationnelle du SCRS.

Le Comité est l'un des mécanismes conçus pour assurer la reddition de comptes par le SCRS. Celui-ci doit en outre rendre compte de ses opérations par l'entremise de l'appareil gouvernemental en place, notamment le ministre de la Sécurité publique

et de la Protection civile, l'inspecteur général du SCRS, les organismes centraux du gouvernement fédéral et le vérificateur général ainsi que les commissaires à l'information et à la protection de la vie privée du Canada.

ÉTUDES DU CSARS EN 2004-2005

Examen du processus d'inscription des entités terroristes

Rapport nº 2004-03

Le CSARS a effectué en 2004-2005 sa première étude d'un rôle que la nouvelle *Loi antiterroriste* du Canada a conféré au SCRS, soit celui que joue le Service dans le processus d'inscription des entités terroristes (IET[1]).

L'étude du Comité a permis de cerner deux questions principales :

Le CSARS a effectué en 2004-2005 sa première étude d'un rôle que la nouvelle *Loi antiterroriste* du Canada a conféré au SCRS.

- l'autorisation du SCRS à recueillir des informations pour le processus d'IET et l'étendue de ses activités de collecte;
- les contraintes entourant la capacité du CSARS à effectuer une étude approfondie du processus d'inscription.

Autorisation du SCRS à prendre part au processus d'inscription

Le mandat concernant le processus d'IET est conféré par l'article 83.05 du *Code criminel* modifié par la *Loi antiterroriste*. Le rôle du SCRS dans ce processus est d'élaborer des rapports de renseignements de sécurité (RRS) dont le ministre de la Sécurité publique et de la Protection civile tient compte au moment de recommander ou non l'inscription d'une entité au gouverneur en conseil.

Lorsque le Comité a examiné le rôle du SCRS dans le processus d'IET, voici les questions qu'il s'est posées :

- *D'où le Service tient-il l'autorisation de prendre part au processus d'IET?*
- *Que signifie « menaces envers la sécurité du Canada », selon la définition énoncée à l'article 2 de la* Loi sur le SCRS?
- *La définition de « menaces envers la sécurité du Canada », dans la* Loi sur le SCRS, *est-elle conforme à celle d'« activité terroriste », du* Code criminel?

1. Dans le *Code criminel* figure uniquement le terme « liste d'entités ». Le sigle IET est employé strictement pour aider le lecteur.

Précisions sur le processus d'inscription des entités terroristes au Canada

La législation canadienne prévoit deux mécanismes pour l'inscription des terroristes, dans le *Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme (RARNULT)* ou dans le *Code criminel* fédéral modifié par la *Loi antiterroriste*.

Le nom d'une personne ou d'un groupe est porté sur la liste prévue au *RARNULT* si le Conseil de sécurité des Nations Unies convient de l'inscrire en vertu du *Règlement d'application des résolutions des Nations Unies sur l'Afghanistan*, qui autorise l'inscription des individus ou groupes associés au Taliban ou à Oussama ben Laden. En qualité de membre de l'ONU, le Canada procède d'office à l'inscription. Autrement, le nom d'une personne ou d'un groupe peut être porté sur la liste canadienne prévue au *RARNULT*, sur la foi d'une recommandation d'Affaires étrangères Canada. Ce processus s'amorce généralement lorsqu'un autre pays notifie son intention d'inscrire une entité terroriste à ce ministère. Celui-ci convoque une réunion interministérielle pour examiner l'inscription proposée et formule sa recommandation au gouverneur en conseil. La liste du *RARNULT* compte actuellement plus de 480 noms.

Selon le processus prévu au *Code criminel*, les noms dont l'inscription proposée est soumise à étude sont l'aboutissement d'une consultation interministérielle au sein du gouvernement du Canada. Lorsque le nom d'une entité est proposé, le SCRS prépare à son sujet un rapport de renseignements de sécurité (RRS). Le ministre de la Sécurité publique et de la Protection civile (SPPC) étudie ce rapport et fait une recommandation au gouverneur en conseil quant à savoir si l'entité doit être inscrite ou non. Cette liste compte près de 40 noms.

L'inscription comporte de graves conséquences. Quiconque est reconnu coupable d'effectuer sciemment, directement ou indirectement, une opération portant sur un bien appartenant à une organisation terroriste ou contrôlé par elle ou pour son compte, est passible d'une amende maximale de 100 000 $ et d'un emprisonnement maximal de 10 ans. Le Bureau du surintendant des institutions financières tient sur son site Web (www.osfi-bsif.gc.ca) une liste d'entités regroupant les noms de toutes les personnes et entités qui figurent sur les listes prévues par le *Code criminel* et le *RARNULT*. Les institutions financières sont tenues de vérifier constamment si les noms de personnes inscrites sur cette liste combinée figurent dans leurs dossiers et de signaler leurs constatations sur-le-champ à la fois à la GRC et au SCRS.

Il était nécessaire de poser ces questions, car plusieurs entités (35 groupes au 31 mars 2005) figurant sur la liste prévue au *Code criminel* ne semblent pas visées par la définition de « menaces envers la sécurité du Canada », de la *Loi sur le SCRS*. Par exemple, la secte japonaise Aum Shinrikyo et Autodefensas Unidas de Colombia (Autodéfenses unies de Colombie) sont toutes deux inscrites à titre d'entités terroristes, mais aucune n'a commis d'acte terroriste en territoire canadien et n'y a une présence manifeste ou un appareil de soutien.

L'objectif de la *Loi antiterroriste* est d'harmoniser les lois du Canada avec celles de ses partenaires étrangers. Mais la *Loi sur le SCRS* ne comporte pas cette dimension internationale du processus d'inscription.

L'article 2 de la *Loi sur le SCRS* est très explicite en raison de l'importance que le Parlement attachait au fait de circonscrire clairement dans la loi les activités du Service en matière de collecte. On y définit « menaces envers la sécurité du Canada » comme étant les activités « visant le Canada » ou « préjudiciables à ses intérêts » (*2a*); celles « qui touchent le Canada ou s'y déroulent » (*2b*, *2c*); ou les activités « qui [...] visent à saper le régime de gouvernement constitutionnellement établi au Canada » (*2d*). Le Canada et ses intérêts sont le dénominateur commun aux quatre définitions de « menaces envers la sécurité du Canada ».

Par contre, l'article 83.01 du *Code criminel* définit « activité terroriste » comme une « action ou omission », figurant parmi les infractions énumérées, qui est commise « au Canada ou à l'étranger ». La *Loi sur le SCRS* établit expressément un lien particulier avec le Canada (soit « qui touchent le Canada ou s'y déroulent »), mais selon la définition d'activité terroriste, énoncée dans le *Code criminel*, celle-ci peut toucher ou non le Canada, car la définition englobe des activités qui peuvent être exercées « à l'étranger » et qui n'ont pas besoin de toucher expressément le Canada. Il n'est pas nécessaire qu'une activité terroriste soit clairement liée au Canada pour être visée par la définition d'« activité terroriste » selon le *Code criminel*.

Comme l'a affirmé le ministère de la Justice, l'objectif de la *Loi antiterroriste* est d'harmoniser les lois du Canada avec celles de ses partenaires étrangers[2]. Mais après étude, le Comité a noté que la *Loi sur le SCRS* ne comporte pas cette dimension internationale du processus d'inscription, ayant pour objet de limiter les activités de collecte du Service aux préoccupations d'ordre national.

2. Voir la fiche d'information du ministère de la Justice, « *Loi antiterroriste* proposée par le Canada : œuvrer avec nos partenaires internationaux », http://www.canada.justice.gc.ca/fr/news/nr/2001/doc_27791.html (dernière mise à jour : 25 avril 2003).

Ce que cela signifie dans l'optique du CSARS

Le Comité soutient que le processus d'inscription peut obliger le SCRS à recueillir, à conserver et à analyser des informations étrangères à la définition de « menaces envers la sécurité du Canada » selon la *Loi sur le SCRS*.

Activités de collecte, d'analyse et de conservation pour le processus d'IET
Activités autorisées selon la *Loi sur le SCRS*

Figure 1 Les activités d'enquête du SCRS s'insèrent dans deux cercles concentriques.

Par analogie, le pouvoir du SCRS d'enquêter sur les menaces s'insère dans deux cercles concentriques. Le cercle intérieur, plus petit, représente les activités du Service autorisées à l'article 12 et limitées aux « menaces envers la sécurité du Canada ». Le cercle extérieur, sensiblement plus grand, représente celles qui ont trait à la collecte, à l'analyse et à la conservation d'information et de renseignements relatifs à toute « activité terroriste » pour le processus d'IET, ainsi que les conseils du SCRS à ce sujet, selon le mandat conféré par le *Code criminel*.

Une bonne partie de l'information contenue dans ces deux cercles coïncide et entre dans le mandat du Service selon la *Loi sur le SCRS*. Mais, après s'être penché sur la question, le Comité a conclu qu'il y a un secteur où les deux cercles ne coïncident pas.

Le CSARS reconnaît que la loi autorise le SCRS à recueillir des informations et des renseignements pour le processus d'IET, suivant les instructions reçues du Ministre. Ces instructions ne peuvent toutefois pas élargir le mandat du Service. Elles ne peuvent que lui conférer le pouvoir de circonscrire ses activités dans les limites déjà définies dans la *Loi sur le SCRS*.

> Le Comité a néanmoins conclu que le processus obligeait le Service à recueillir certains renseignements qui débordent les pouvoirs énoncés dans la *Loi sur le SCRS*, en ce qui a trait aux « menaces envers la sécurité du Canada ».

Dans l'ensemble de son étude sur le rôle du Service à l'égard du processus d'IET, le CSARS a constaté que la collecte d'informations destinées à ce processus, par le SCRS, avait été conforme aux instructions ministérielles, une fois que celles-ci lui eurent été données[3], et aux politiques opérationnelles pertinentes. Le Comité a néanmoins conclu

3. Le CSARS note que, pendant la première année du processus d'IET, le SCRS a exercé ses nouvelles fonctions sans instruction officielle du Ministre. Les Exigences nationales en matière de renseignement de sécurité (2003-2004) sont entrées en vigueur le 1er avril 2003, quinze mois après l'adoption de la *Loi antiterroriste*.

que le processus obligeait le Service à recueillir certains renseignements qui débordent les pouvoirs énoncés dans la *Loi sur le SCRS*, en ce qui a trait aux « menaces envers la sécurité du Canada ».

Cet élargissement des activités de collecte du SCRS et l'absence d'autorisation claire à leur égard préoccupent le CSARS. Après tout, l'intention du Parlement était que ces activités soient définies avec précision en raison des pouvoirs extraordinaires du Service.

Capacité du CSARS à examiner le rôle du Service dans le processus d'IET

Le Comité sénatorial spécial qui, le premier, a examiné le projet de loi C-36 (*Loi antiterroriste*) a déploré l'absence de dispositions satisfaisantes permettant une surveillance indépendante du processus d'IET. Les sénateurs se sont tout particulièrement inquiétés de la participation du SCRS à l'examen biennal de la liste, notant que celle-ci serait effectivement étudiée par les personnes mêmes qui l'ont dressée[4]. En conséquence, ils ont recommandé ou bien qu'un poste de haut fonctionnaire du Parlement soit créé pour surveiller le processus d'IET ou bien que le CSARS soit chargé d'en assurer l'examen biennal[5].

> Même si le CSARS peut faire une étude assez complète du rôle du Service dans le processus d'IET, il ne peut l'évaluer entièrement puisqu'il n'est pas autorisé à prendre connaissance des rapports de renseignements de sécurité qui fondent les décisions du gouverneur en conseil, du fait qu'il s'agit de renseignements confidentiels du Cabinet.

À ce moment-là, la ministre de la Sécurité publique et de la Protection civile (alors ministre de la Justice et procureure générale du Canada) a soutenu que les mécanismes de surveillance existants étaient satisfaisants, affirmant ceci : « nous avons des mécanismes de surveillance en place qui ont fait leurs preuves, que ce soit le CSARS ou les tribunaux. Par conséquent, je ne suis pas favorable à la création d'un nouveau mécanisme de surveillance distinct et séparé de ceux qui existent[6] ».

En février 2005, les sénateurs ont à nouveau exprimé leurs inquiétudes à la Ministre (de la Sécurité publique et de la Protection civile) lors de son témoignage devant le Comité sénatorial spécial sur la *Loi antiterroriste*. Elle a de nouveau qualifié le CSARS

4. La ministre de SPPC a terminé son premier examen de la liste d'entités, prévu par la loi, le 16 novembre 2004.
5. Comité sénatorial spécial sur la teneur du projet de loi C-36, Premier rapport (1er novembre 2001), page 5.
6. Honorable Anne McLellan, témoignage devant le Comité sénatorial spécial sur la teneur du projet de loi C-36 (29 octobre 2001). Elle a aussi affirmé : « il existe maintenant des instances de surveillance. Vous avez mentionné le CSARS. Celui-ci assumera toute nouvelle obligation en tant que instance de surveillance des activités du SCRS dans le cadre de cet effort concerté visant à éradiquer et à prévenir les activités terroristes ».

d'un des « importants mécanismes de protection et de reddition de comptes » dans le cadre de la *Loi antiterroriste*[7].

Comme la Ministre a qualifié expressément d'important mécanisme de protection la capacité du CSARS à examiner la liste, celui-ci estime important de noter que, même s'il peut faire une étude assez complète du rôle du Service dans le processus d'IET, il ne peut l'évaluer entièrement puisqu'il n'est pas autorisé à prendre connaissance des rapports de renseignements de sécurité qui fondent les décisions du gouverneur en conseil, du fait qu'il s'agit de renseignements confidentiels du Cabinet. Le Comité admet qu'il ne peut prendre connaissance des documents confidentiels du Cabinet en raison du paragraphe 39(3) de la *Loi sur le SCRS*. Cependant, dans les rares occasions où il s'est heurté par le passé au problème de l'accès à ces documents, il s'est entendu avec les solliciteurs généraux en poste de manière à apaiser ses craintes.

Une autre préoccupation, bien que moins grave celle-là, au sujet de l'examen du processus d'IET par le CSARS est qu'un autre organisme, comme la GRC, pourrait préparer un rapport de renseignements de sécurité. L'article du *Code criminel*, qui traite de l'examen judiciaire du processus d'inscription, fait état des « renseignements en matière de sécurité ou de criminalité qui ont été pris en considération pour l'inscription du demandeur » (83.05 (6)*a*), mais il ne précise pas quel ministère ou organisme canadien peut préparer ces rapports. La mention de « criminalité » donne à penser que la GRC pourrait jouer un rôle dans ce processus.

Si la GRC venait à préparer un rapport de renseignements de sécurité destiné à être soumis au gouverneur en conseil dans le processus d'IET, le Comité n'aurait pas compétence pour examiner l'affaire puisque son mandat se limite à l'activité du SCRS.

Au sujet de la question des documents confidentiels du Cabinet, les membres du CSARS l'ont soulevée directement auprès de la Ministre lorsqu'ils l'ont rencontrée, en février 2005.

Actions du CSARS

Au sujet de la question des documents confidentiels du Cabinet, les membres du CSARS l'ont soulevée directement auprès de la Ministre lorsqu'ils l'ont rencontrée, en février 2005. Le Comité a aussi résumé ses préoccupations dans deux lettres qu'il lui a adressées en décembre 2004 et en mars 2005. Ses membres ont étayé ces craintes le 18 avril 2005, devant le Comité sénatorial spécial sur la *Loi antiterroriste*, et le 8 juin 2005, devant le sous-comité de la Chambre. **Le CSARS est déçu de noter qu'il n'avait pas encore reçu de réponse au moment de mettre sous presse.**

7. Honorable Anne McLellan, témoignage devant le Comité sénatorial spécial sur la *Loi antiterroriste* (14 février 2005).

Collecte, analyse et conservation de renseignements sur les menaces envers la sécurité du Canada

Le Service tient principalement des articles 2 et 12 de la *Loi sur le SCRS* son pouvoir de recueillir, d'analyser et de conserver des informations et renseignements. Presque chacune des études du CSARS comporte un volet essentiel qui consiste à déterminer si le Service a exercé ses fonctions conformément à ces deux articles.

L'article 12 de la *Loi* se lit ainsi :

Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.

L'article 2 de la *Loi* définit menaces en ces termes :

a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;

b) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;

c) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger;

d) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence.

Les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord sont expressément exclues, sauf si elles sont exercées en même temps que les menaces énumérées.

Dans son premier rapport sur le projet de loi C-36, le Comité sénatorial a dit craindre, au sujet de la liste, que « le fait d'y inscrire erronément le nom d'une personne ou d'un groupe ne cause un préjudice irréparable à la réputation des intéressés[8] ». Le CSARS reconnaît les importantes questions que pose le processus d'IET sur le plan des libertés civiles et il prend au sérieux les craintes soulevées par cette étude.

Étude de l'enquête du SCRS sur la criminalité transnationale

Rapport nº 2004-02

Contexte

Cette étude visait à évaluer l'enquête du SCRS sur la criminalité transnationale (CT) et portait sur les activités menées au Canada par plusieurs organisations criminelles transnationales étrangères. C'est la deuxième étude du CSARS sur la question, depuis le rapport nº 107, publié en 1998 (SIRC 1998-01).

En 1995, les États membres du G7 (dont le Canada) ont convenu de reconnaître la criminalité transnationale comme une menace à la sécurité nationale. Depuis 1996, le solliciteur général du Canada (maintenant appelé ministre de la Sécurité publique et de la Protection civile) dicte au SCRS d'enquêter sur la CT, dans le cadre de ses exigences nationales annuelles en matière de renseignement de sécurité. La CT est donc un sujet de préoccupation dans la planification annuelle du Service en matière de contre-espionnage (CE) depuis 1995-1996. Les enquêtes sont menées par les Sous-sections de la CT, rattachées à la Direction du contre-espionnage, qui sont disséminées dans les diverses régions du Canada.

Les enquêtes choisies pour cette étude, de portée nationale, étaient autorisées aux niveaux II et III et portaient sur de présumées activités constituant des menaces décrites à l'alinéa 2*b*) de la *Loi sur le SCRS*. Cet alinéa définit le rôle du Service en matière de renseignement relativement à la CT. Dans l'étude précédente, le CSARS a fait valoir la nécessité que le SCRS établisse avec soin une distinction entre son rôle à l'égard de la sécurité nationale et les enquêtes criminelles menées par les organismes d'application de la loi[9]. Dans la présente étude, il a été attentif à cette constatation.

8. Comité sénatorial spécial sur la teneur du projet de loi C-36, Premier rapport (1er novembre 2001), page 5.
9. Rapport annuel du CSARS 1998-1999, page 7.

Méthode

L'étude a été menée d'après le mandat conféré au Comité selon l'alinéa 38*b*) et l'article 40 de la *Loi sur le SCRS*. Le CSARS a choisi une période d'étude de huit mois, allant du 1er septembre 2002 au 30 avril 2003, et il a examiné une liste des cibles du Service liées à la CT pour choisir une autorisation d'enquête contextuelle et quatre cibles. Cela lui a fourni l'occasion d'examiner divers processus de ciblage exposés dans la politique opérationnelle, y compris le lancement d'une nouvelle enquête, un renouvellement et le relèvement (de II à III) du niveau d'une enquête.

L'étude visait à répondre aux questions suivantes :

- Le Service avait-il des motifs raisonnables de soupçonner l'existence d'une menace envers la sécurité du Canada?
- Le niveau de l'enquête et son degré d'intrusion étaient-ils proportionnels à la gravité et à l'imminence de la menace?
- Le SCRS a-t-il recueilli uniquement des informations strictement nécessaires pour remplir son mandat d'informer le gouvernement de l'existence d'une menace?
- Les échanges d'information avec des organismes canadiens et étrangers étaient-ils conformes aux articles 13 et 17 de la *Loi sur le SCRS* ainsi qu'aux politiques opérationnelles?

Pour répondre à ces questions, le CSARS a examiné tous les rapports de la période à l'étude, versions papier et électronique, et il en a évalué la conformité à la *Loi sur le SCRS*, aux instructions ministérielles, aux Exigences nationales et à la politique opérationnelle. Plus précisément, il s'est penché sur :

- les décisions de ciblage et les enquêtes correspondant à un échantillon de cibles;
- les demandes d'autorisation d'enquête et les rapports opérationnels justificatifs;
- la coopération et les échanges d'information avec les partenaires canadiens et étrangers.

Constatations

Le Comité a conclu que le SCRS avait raison de croire que les activités des quatre cibles individuelles étaient dirigées par l'étranger ou menées au nom d'intérêts étrangers, et présentaient généralement une menace au sens de la définition de l'alinéa 2*b*) de la *Loi sur le SCRS*. Qui plus est, il a constaté que le Service avait respecté en tous points les instructions ministérielles et la politique opérationnelle dans ses demandes d'autorisation d'enquête. Le SCRS a en outre pratiqué un degré d'intrusion proportionnel aux menaces présumées.

Dans l'ensemble, les opérations examinées ont été menées conformément à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle et les méthodes employées par le Service concordaient avec les niveaux d'enquête approuvés.

L'article 12 de la *Loi sur le SCRS* autorise la collecte d'informations sur des menaces présumées à l'égard de la sécurité du pays. Le Service conseille alors le gouvernement du Canada au sujet des activités qui peuvent être soupçonnées de menacer la sécurité nationale. Le CSARS a trouvé que la vaste majorité des informations recueillies par le SCRS sur la CT durant la période à l'étude étaient effectivement strictement nécessaires à l'exécution de son mandat.

Dans l'ensemble, les opérations examinées ont été menées conformément à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle et les méthodes employées par le Service concordaient avec les niveaux d'enquête approuvés.

Cependant, le CSARS a relevé un cas où des informations recueillies en vertu de l'article 15 de la *Loi sur le SCRS* avaient été transférées à tort à une enquête en vertu de l'article 12. L'article 15 autorise le Service à mener les enquêtes requises pour fournir des évaluations de sécurité. Le Comité déplore que le transfert d'information recueillie initialement lors d'une entrevue suivant l'article 15 ne respectait pas toujours le critère de « la mesure strictement nécessaire ». Il estime que, dans ce cas-là, le Service a transféré sans nécessité, des renseignements personnels et professionnels et des données d'emploi, d'une entrevue en vertu de l'article 15 à des rapports opérationnels de l'enquête sur la CT en vertu de l'article 12.

La personne interviewée n'étant pas une cible, le Comité a conclu que ces rapports débordaient les exigences raisonnables quant aux données de base et au contexte. Il compte suivre les rapports opérationnels de l'information recueillie lors d'entrevues en vertu de l'article 15 pour assurer que le Service respecte la *Loi sur le SCRS* et sa politique opérationnelle.

Dans son étude de 1998, le Comité avait conclu « qu'on n'avait [pas] bien défini les critères permettant de distinguer renseignements stratégiques et renseignements tactiques », ce qui avait amené le SCRS à recueillir et à conserver de l'information sur « des activités criminelles tactiques, menées en milieu urbain et débordant manifestement ses objectifs stratégiques[10] ».

10. Rapport annuel du CSARS 1998-1999, page 7.

Dans cette étude, le Comité a constaté que le Service avait amélioré considérablement ses pratiques d'enquête dans le domaine de la criminalité transnationale et qu'il y avait relativement peu de cas de collecte ou de conservation de renseignements tactiques.

Les renseignements relatifs aux enquêtes criminelles ont été fournis aux organismes d'application de la loi conformément à l'article 17 de la *Loi sur le SCRS*. De même, les échanges avec des organismes étrangers étaient dans le champ des ententes conclues avec eux. Le CSARS a constaté que les échanges d'information entre le Service et ses partenaires canadiens et étrangers comportaient les mises en garde requises. De plus, ils étaient conformes à la politique opérationnelle et aux protocoles d'entente pertinents.

Enquêtes

Le SCRS établit le niveau d'une enquête à mener sur les activités de personnes ou d'organismes s'il a des motifs raisonnables de soupçonner que ces activités menacent la sécurité du Canada. Les conditions d'approbation du niveau d'enquête sont exposées en détail dans la politique opérationnelle. C'est le Comité d'approbation et de réévaluation des cibles qui est investi du pouvoir d'administrer, d'étudier et d'approuver les demandes de niveaux d'enquête. Il est présidé par le directeur du SCRS et composé de plusieurs cadres supérieurs du Service, de l'avocat général (ministère de la Justice) et d'un représentant du sous-ministre de la Sécurité publique et de la Protection civile.

Il existe trois niveaux d'enquête :

Niveau I

- Permet d'utiliser les techniques comportant le moins d'intrusion. Les enquêtes de niveau I sont instituées pour des périodes brèves et permettent au SCRS de recueillir de l'information auprès de sources ouvertes et dans les documents des services de police ou des organismes de sécurité ou de renseignement canadiens et étrangers.

Niveau II

- Permet de recourir à des techniques comportant un degré modéré d'intrusion. Les enquêtes de niveau II peuvent comporter des entrevues personnelles et une filature limitée.

Niveau III

- Permet d'utiliser les techniques comportant l'intrusion la plus poussée, comme on peut le voir à l'article 21 de la *Loi sur le SCRS*. Le recours à ces techniques est assujetti aux contrôles judiciaires les plus stricts.

Dans son étude de l'enquête contextuelle, le Comité a relevé une série d'événements qui ont révélé un recours particulièrement efficace aux ententes avec des organismes canadiens et étrangers. En l'occurrence, le Service a jugé que certaines informations reçues d'un organisme canadien constituaient une menace pour la vie d'une personne. Même s'il n'était pas tenu de le faire, il s'est empressé d'en obtenir l'autorisation de communiquer les informations pertinentes à un service étranger partenaire, ce qu'il a fait. En agissant ainsi, il se peut qu'il ait contré un attentat à la vie de l'intéressé.

Le Comité a constaté que le Service avait amélioré considérablement ses pratiques d'enquête dans le domaine de la criminalité transnationale et qu'il y avait relativement peu de cas de collecte ou de conservation de renseignements tactiques.

Cette étude n'a donné lieu à aucune recommandation.

Étude d'une enquête antiterroriste

Rapport nº 2004-05

Contexte

Pour cette étude, le CSARS a examiné une enquête antiterroriste menée par le SCRS, dont il n'avait fait aucune étude exhaustive depuis plus de dix ans et qui demeurait pourtant hautement prioritaire à la Direction de l'antiterrorisme. Cette enquête était l'objet d'une autorisation de niveau III à l'égard de présumées activités constituant des menaces décrites à l'alinéa 2*c*) de la *Loi sur le SCRS*.

Méthode

Le CSARS a d'abord examiné les listes de toutes les cibles et sources humaines du SCRS et de tous les mandats, reliés à son enquête. Il a ensuite choisi pour objet d'une étude approfondie la cible d'une enquête contextuelle, un organisme ciblé, six cibles individuelles, un mandat et six opérations ayant fait appel à des sources humaines. Dans chaque dossier, tous les documents en versions électronique et imprimée ont été étudiés pour la période du 1er janvier au 31 décembre 2003. Pour être sûr d'aller au fond des choses, le CSARS a aussi scruté certains documents hors de cette période.

Comme dans les autres études d'enquêtes du Service, le CSARS a évalué dans quelle mesure celui-ci s'était conformé à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle, en examinant des activités d'ordre opérationnel clés :

- les décisions de ciblage et les enquêtes;
- la demande et l'exercice de pouvoirs conférés par mandat et les opérations spéciales;
- la gestion des sources humaines et des opérations délicates;
- la coopération et les échanges d'information avec les partenaires canadiens;
- la coopération et les échanges d'information avec les partenaires étrangers;
- les conseils donnés au gouvernement.

Le CSARS a cherché à déterminer :

- si le Service avait des motifs raisonnables de soupçonner l'existence d'une menace à l'égard de la sécurité du Canada;
- si le niveau des enquêtes et leur degré d'intrusion étaient proportionnels à la gravité et à l'imminence de la menace;
- si le SCRS avait recueilli uniquement des informations strictement nécessaires pour remplir son mandat d'informer le gouvernement de l'existence d'une menace.

Constatations

Le Comité a constaté que, d'après les renseignements dont disposait le Service, celui-ci avait des motifs raisonnables de soupçonner les cibles d'enquête de constituer une menace pour la sécurité du Canada. Le niveau et le degré d'intrusion des enquêtes du SCRS étaient proportionnels à la menace présumée.

Le CSARS a cherché à clarifier pourquoi un individu était toujours la cible d'une enquête plusieurs mois après son départ du Canada. L'explication du Service l'a convaincu que le délai à clore l'enquête sur cette cible était raisonnable.

Le CSARS a cherché à clarifier pourquoi un individu était toujours la cible d'une enquête plusieurs mois après son départ du Canada.

Dans l'ensemble, les activités du Service étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Il n'a recueilli que les informations qui lui étaient strictement nécessaires pour remplir son mandat.

Le Service a satisfait à toutes les exigences de la *Loi sur le SCRS* et de la politique opérationnelle quant à l'obtention de mandats. Le CSARS a constaté que le Service avait les informations requises pour justifier tous les énoncés factuels de l'affidavit.

De plus, celui-ci était complet et équilibré, les faits et circonstances du dossier étant exposés de manière fidèle, juste et objective.

Le CSARS a constaté que, dans l'exercice des pouvoirs autorisés par le mandat, le Service s'était conformé à la *Loi sur le SCRS*, à la politique opérationnelle et aux conditions imposées par la Cour fédérale. Cependant, il a constaté que l'orientation fournie dans la politique opérationnelle existante n'était pas suffisante quant à certaines procédures administratives entourant l'exercice de quelques-uns de ces pouvoirs. Le Service lui a fait part de l'approbation de nouvelles dispositions à la politique opérationnelle pour combler cette lacune. Le Comité a aussi assuré le suivi d'un problème, relevé dans son étude nº 2003-04, concernant la non-conformité d'un bureau régional du SCRS à la politique opérationnelle. L'enquête visée n'a révélé aucun problème de cette nature.

Le CSARS a constaté que l'orientation fournie dans la politique opérationnelle existante n'était pas suffisante quant à certaines procédures administratives entourant l'exercice de quelques-uns de ces pouvoirs.

Les opérations faisant appel à des sources humaines ont été bien gérées par le Service et étaient pleinement conformes aux instructions ministérielles et à la politique opérationnelle. Les dossiers administratifs et financiers de chaque opération étaient en bon ordre. De plus, le CSARS a constaté que le SCRS avait géré judicieusement les relations avec les sources auxquelles il avait eu recours dans les domaines délicats.

Avec en arrière-fond les lois en évolution, le Comité a aussi évalué les politiques du Service relatives aux opérations qui font appel à des sources humaines afin de déterminer si elles étaient satisfaisantes, et il a constaté qu'elles l'étaient. Il continuera à suivre de près cette activité opérationnelle dans ses futures études.

Le Comité n'a cerné aucun problème ni préoccupation au sujet des rapports du Service avec ses partenaires canadiens et étrangers. Les échanges d'information avec eux étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Le CSARS a porté à l'attention du Service un petit nombre d'erreurs ou omissions administratives, relevées dans les rapports opérationnels. Celui-ci les a par la suite corrigées.

Enfin, le Comité a donné suite à une question observée dans son étude nº 2003-02 au sujet des implications de la *Loi antiterroriste*. Il avait alors eu des craintes à l'égard de la rétribution des sources humaines. Le CSARS a demandé au Service s'il avait revu

Autorisations contextuelles

Ce type d'autorisations permet au Service de faire enquête dans les circonstances où il soupçonne l'existence d'une menace pour la sécurité du Canada, mais où il ne connaît pas encore les personnes ou groupes particuliers qui sont associés à cette menace. Comme dans toute autre procédure d'autorisation, s'il faut demander des pouvoirs octroyés par mandat, l'autorisation doit émaner de la Cour fédérale du Canada. Selon la politique opérationnelle, le SCRS doit demander une autorisation d'enquête distincte dès qu'il apprend que des groupes, personnes ou organisations prennent part à des activités liées à la menace relativement à un contexte ou à un événement.

Au Comité, il demeure d'usage courant d'évaluer au cas par cas chacune des enquêtes contextuelles de façon à s'assurer qu'elles sont menées dans les règles.

ses politiques ou lignes directrices concernant cette rétribution. En réponse, le SCRS l'a informé d'un avis juridique reçu, indiquant que son approche était bonne.

Lors d'études futures, le CSARS compte suivre les opérations du Service qui font appel à des sources humaines et mettent en cause des entités terroristes inscrites, afin de cerner toute préoccupation et de réévaluer si la politique opérationnelle est satisfaisante à cet égard. Cette étude n'a donné lieu à aucune recommandation.

Examen des activités et enquêtes d'un bureau régional du SCRS

Rapport nº 2004-04

Contexte

Chaque année, le CSARS s'efforce de faire un examen global des activités du SCRS dans une région particulière du Canada. Ce type d'étude englobe en général le ciblage d'individus, l'exercice de pouvoirs conférés par mandat, le recours à des sources humaines ainsi que la coopération et les échanges d'information avec les partenaires canadiens et étrangers. Pareille étude fournit un éclairage unique sur la manière dont le SCRS emploie les divers outils d'enquête dont il dispose, outre le fait qu'elle permet normalement d'évaluer s'il respecte la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle.

Méthode

Le CSARS a choisi un bureau régional et en a examiné les activités pour la période du 1er avril 2002 au 31 mars 2003. En premier lieu, il a étudié les données préliminaires sur toutes les enquêtes actives en 2002-2003. À partir de là, il a décidé d'axer son examen sur une enquête antiterroriste particulière dont l'objet est devenu la lutte contre la prolifération en juillet 2002.

Le CSARS a examiné tous les documents de la période à l'étude, versions papier et électronique, concernant cinq types d'activités du SCRS sur le plan opérationnel :

- le ciblage d'individus soupçonnés d'exercer des activités constituant des menaces, et le processus d'autorisation d'enquête;
- l'exercice des pouvoirs conférés par mandat contre les cibles autorisées;
- les opérations spéciales donnant lieu à l'exercice de pouvoirs conférés par mandat;
- la direction de sources humaines contre les cibles autorisées;
- les échanges d'information avec d'autres organismes canadiens et étrangers d'application de la loi et de renseignement de sécurité.

Le CSARS a aussi examiné les mesures de sécurité interne du SCRS dans la région, ainsi que les manquements et les infractions à la sécurité entre le 1er avril 2000 et le 31 mars 2003.

Comme dans toutes les études, le CSARS a cherché à répondre à trois questions principales :

- Le SCRS avait-il des motifs raisonnables de soupçonner l'existence d'une menace à l'égard de la sécurité du Canada?
- Le niveau de l'autorisation d'enquête était-il proportionnel à la menace?
- Le Service a-t-il recueilli uniquement des informations strictement nécessaires à son enquête?

Le CSARS s'est rendu sur place pour mieux saisir la nature des opérations régionales et les défis uniques auxquels faisaient face les enquêteurs du Service dans la région à l'étude.

Constatations

Dans l'ensemble, les activités de la région en matière d'enquête au cours de la période à l'étude étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Le CSARS a constaté que le Service avait des motifs raisonnables de soupçonner les cibles d'enquête autorisées de constituer une menace pour la sécurité du Canada et que le degré d'intrusion des méthodes employées était proportionnel à la menace présumée, présentée par ces cibles.

Les pouvoirs conférés par mandat, tel celui d'intercepter les appels téléphoniques, figurent parmi les techniques d'enquête les plus intrusives dont dispose le SCRS. Ils sont conférés par la Cour fédérale du Canada. Le CSARS a constaté que le Service s'était conformé aux conditions imposées dans le mandat de la Cour fédérale pour l'exercice des pouvoirs conférés par elle et pour la conduite d'opérations spéciales au cours de la période à l'étude. Le SCRS a exercé ces pouvoirs uniquement s'ils étaient nécessaires pour pousser son enquête plus loin. Il n'a pas demandé de renouvellement lorsque les autres pouvoirs prévus dans l'autorisation d'enquête étaient suffisants. Le Service a aussi agi d'une manière irréprochable et conforme à la loi dans la direction des sources humaines et dans l'échange d'information avec d'autres organismes.

L'attention du CSARS a porté sur la participation de certaines cibles au sein d'un organisme local qui avait de multiples fonctions. Le SCRS a évalué que certaines activités en cours ne constituaient pas un volet important de l'organisme, estimant que celui-ci nourrissait principalement un objectif. Le CSARS estime que la politique opérationnelle régissant certains types d'enquêtes devrait s'appliquer à cet organisme. Le SCRS s'est dit en désaccord avec cette constatation.

L'article 12 de la *Loi sur le SCRS* limite celui-ci à recueillir des informations « dans la mesure strictement nécessaire » pour ses enquêtes sur les activités qui constituent des menaces. Le CSARS a constaté qu'en général le Service avait amassé uniquement des informations strictement nécessaires à son enquête. Il estime cependant que, dans un cas, le SCRS a recueilli et consigné dans un rapport des renseignements personnels qui frisent la limite du permis selon la *Loi*.

Au fil de l'étude, l'attention du CSARS a porté sur la participation de certaines cibles au sein d'un organisme local qui avait de multiples fonctions. Le SCRS a évalué que certaines activités en cours ne constituaient pas un volet important de l'organisme, estimant que celui-ci nourrissait principalement un objectif.

Le Comité a examiné avec soin tous les documents où figurait le nom de l'organisme. Il s'est aussi penché sur l'information au dossier, provenant d'une étude antérieure de la même enquête. Cela lui a permis de constater que l'organisme avait une double fonction.

Le CSARS estime que la politique opérationnelle régissant certains types d'enquêtes devrait s'appliquer à cet organisme. Le SCRS s'est dit en désaccord avec cette constatation.

Le Comité reconnaît qu'en pareille situation il peut être difficile de déterminer quelles dispositions de la politique opérationnelle s'appliquent. Aussi a-t-il recommandé que le SCRS définisse un terme particulier de cette politique.

Le Comité a aussi trouvé un cas où le SCRS ne s'était pas conformé en tous points à la politique opérationnelle. Celui-ci s'est dit en désaccord. Outre ces problèmes, le CSARS a relevé quelques erreurs administratives dans l'exercice des pouvoirs conférés au Service par mandat, le recours aux sources humaines et les échanges d'information. Ces erreurs étaient bénignes et n'ont pas affecté les enquêtes du SCRS. De plus, le Comité a été informé que celui-ci avait fait des changements pour éviter de les répéter.

Aussi à noter, le Comité a examiné les pratiques et procédures de sécurité qui étaient en place depuis 2000 dans la région à l'étude. Une infraction à la sécurité a fait l'objet d'une plainte connexe sur laquelle il a enquêté conformément à l'article 42 de la *Loi sur le SCRS*[11].

Étude d'une enquête en matière de lutte contre la prolifération

Rapport n° 2004-09

Contexte

En juillet 2002, le Service canadien du renseignement de sécurité a créé la Direction de la lutte contre la prolifération (DLP). Celle-ci regroupe les volets d'enquête qui relevaient préalablement des Directions de l'antiterrorisme (AT) et du contre-espionnage (CE). En 2004, le CSARS a effectué un examen de la DLP. C'était la première occasion qui lui était donnée d'examiner les activités du Service dans la lutte contre la prolifération, sous la nouvelle structure organisationnelle.

Méthode

Cette étude a porté sur l'enquête menée par le Service, entre le 1er janvier 1999 et le 31 décembre 2003, à l'égard de la menace que présentaient pour la sécurité du Canada les activités de personnes ou d'organismes liés à un certain pays, entourant la prolifération d'armes de destruction massive. Pour être sûr d'aller au fond des choses, le CSARS a aussi étudié certains documents débordant cette période.

11. Les manquements à la sécurité sont moins graves que les infractions. Par manquement à la sécurité on entend toute dérogation aux politiques sur la sécurité, comme le fait de ne pas mettre sous clé des renseignements classifiés. Il y a infraction à la sécurité s'il y a divulgation non autorisée d'un renseignement classifié ou accès sans autorisation à un bien classifié.

Le Comité a examiné l'enquête contextuelle du Service. De plus, pour en discuter certains aspects, son personnel a rencontré des représentants de la DLP du SCRS.

Comme dans toutes les études de cette nature, le CSARS a évalué la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle en examinant les principales activités d'ordre opérationnel qui suivent :

- les décisions de ciblage;
- les activités en matière d'enquête et les rapports opérationnels;
- la coopération et les échanges d'information avec des partenaires canadiens;
- la coopération et les échanges d'information avec les partenaires étrangers;
- les conseils au gouvernement fédéral.

Le CSARS a cherché à déterminer :

- si le SCRS avait des motifs raisonnables de soupçonner l'existence d'une menace à l'égard de la sécurité du Canada;
- si le niveau et le degré d'intrusion de l'enquête du Service étaient proportionnels à la gravité et à l'imminence de la menace;
- si le SCRS avait recueilli uniquement des informations strictement nécessaires pour remplir son mandat d'informer le gouvernement de l'existence d'une menace.

Constatations

Le Comité a constaté que le Service s'était conformé en tous points aux instructions ministérielles et à la politique opérationnelle quant aux demandes d'autorisation d'enquête. Les déclarations faites dans les demandes étaient appuyées par les rapports opérationnels du SCRS. Le CSARS a conclu que, d'après les renseignements dont le Service disposait, celui-ci avait des motifs raisonnables de soupçonner chacune des cibles d'enquête autorisées de constituer une menace pour la sécurité du Canada.

Dans l'ensemble, la coopération et les échanges d'information du Service avec les partenaires canadiens et étrangers étaient conformes à la politique opérationnelle.

Le niveau et le degré d'intrusion des enquêtes du Service étaient proportionnels à la menace présumée. Celui-ci n'a recueilli que l'information qui lui était strictement nécessaire pour exécuter son mandat d'informer le gouvernement fédéral au sujet d'une menace.

Le Comité a souscrit à l'approche du Service, à savoir engager des entités compétentes du secteur privé à la faveur du Programme de

liaison et de sensibilisation. Outre le fait que les séances d'information de la DLP au secteur privé aident le SCRS à combler ses besoins opérationnels, elles sont aussi très précieuses pour les bénéficiaires qui pourraient être la cible d'entités étrangères. Ce programme a fourni des pistes à plusieurs reprises et suscité un esprit de coopération chez les représentants de l'industrie.

Dans l'ensemble, la coopération et les échanges d'information du Service avec les partenaires canadiens et étrangers étaient conformes à la politique opérationnelle. Le CSARS n'a décelé aucun problème ni préoccupation au sujet de la coopération du SCRS avec ses partenaires canadiens et étrangers.

Cette étude n'a donné lieu à aucune recommandation.

Examen du Centre des opérations d'information du SCRS

Rapport nº 2004-07

Contexte

En cette ère de l'information, les acteurs hostiles (extrémistes, groupes terroristes, services de renseignement ou forces armées de pays étrangers, p. ex.) n'ont plus besoin d'un accès direct à un ordinateur pour copier, détruire ou manipuler des données. Ils recourent plutôt à divers outils logiciels et techniques pour accéder à distance sans autorisation à un système ciblé et l'exploiter. Ce type d'activité, appelée « opération informatique », peut menacer la sécurité nationale dans certains cas. Pour les responsables des infrastructures essentielles du Canada[12] qui dépendent des réseaux informatiques, il faut être aux aguets de ces attentats. Le Service enquête sur les activités de ceux qui sont soupçonnés de recourir à de telles opérations pour menacer la sécurité du Canada, selon la définition de l'article 2 de la *Loi sur le SCRS*.

Une présumée opération informatique doit répondre à deux critères pour que le SCRS enquête à son sujet :

(1) il doit exister des motifs raisonnables de soupçonner que l'activité concernée est cautionnée par un État étranger (ou l'un de ses mandataires), un groupe terroriste ou des extrémistes d'inspiration politique;

12. Le gouvernement du Canada a déterminé dix secteurs d'infrastructures essentielles : énergie et services publics; communications et technologie de l'information; finances; soins de santé; alimentation; eau; transport; sécurité; gouvernement; et fabrication (Énoncé de position du gouvernement du Canada relativement à une stratégie nationale pour la protection des infrastructures essentielles, novembre 2004).

(2) le but de l'attaque doit avoir trait à l'espionnage, au sabotage, au terrorisme, à des activités influencées par l'étranger ou à la violence visant à atteindre des objectifs politiques, idéologiques ou religieux.

En février 2002, pour contrer la menace que présentaient les attaques sur le Web, le SCRS a créé le Centre des opérations d'information (COI) qui est chargé d'élaborer et d'employer des techniques d'enquête spécialisées.

Méthode

En 2004, le Comité a mené sa toute première étude concernant l'enquête du SCRS sur les menaces aux infrastructures essentielles du Canada en matière d'information, et cela, à deux fins précises. En premier lieu, il a examiné le rôle du COI dans les enquêtes sur les menaces contre les infrastructures essentielles du Canada. Puis, le CSARS s'est penché sur les opérations du COI, vérifiant si une enquête de contre-espionnage au sujet d'une opération informatique était conforme à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle du Service.

En 2004, le Comité a mené sa toute première étude concernant l'enquête du SCRS sur les menaces aux infrastructures essentielles du Canada en matière d'information.

L'étude a couvert la période du 1er janvier 2000 au 31 décembre 2003.

Constatations

Mises à part les deux préoccupations décrites ci-après, le CSARS a constaté que le Service s'était conformé à la *Loi sur le SCRS*, aux instructions ministérielles et à sa politique opérationnelle dans l'exercice de ses fonctions.

La première préoccupation du Comité était que la politique opérationnelle aille de pair avec l'affaire examinée. Le CSARS a recommandé que le Service revoie sa politique opérationnelle concernant les enquêtes menées en ce domaine selon l'article 12.

Le CSARS recommande que le Service revoie sa politique opérationnelle pour assurer qu'elle englobe clairement certaines questions relatives aux enquêtes en vertu de l'article 12.

La deuxième préoccupation du Comité concernait des erreurs administratives : il en a décelé quatre. Trois d'entre elles étaient bénignes, mais l'autre avait trait aux rapports opérationnels du Service, ce qui aurait pu avoir des effets sur le rôle du processus d'autorisation d'enquête à titre de mécanisme redditionnel interne. Le CSARS

a recommandé que le SCRS revoie ses politiques concernant les rapports opérationnels pour éviter de répéter cette erreur.

> **Le CSARS recommande que le Service revoie sa politique opérationnelle pour assurer que, s'il faut renvoyer à des rapports portant un numéro de dossier de la base de données opérationnelles, dans des rapports inscrits sous un autre numéro, cela soit fait dans la partie « Commentaires de l'enquêteur ».**

Le Service a affirmé qu'il examinerait les moyens d'assurer l'établissement de renvois dans les messages de la base de données opérationnelles lorsqu'ils sont transférés d'un dossier d'enquête à un autre.

Examen des échanges d'information du SCRS avec les proches alliés

Rapport nº 2004-08

Contexte

En janvier 2004, le gouvernement fédéral a créé la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar (Commission O'Connor). L'ancien directeur du SCRS, Ward Elcock, s'est porté à la défense des pratiques du Service en matière de partage d'information, notant que le CSARS n'avait critiqué l'à-propos du partage de renseignements avec des services étrangers dans aucun des cas examinés depuis le 11 septembre 2001[13].

L'affaire Arar a toutefois braqué l'attention publique sur l'utilisation de l'information qui pouvait avoir été recueillie au Canada, puis communiquée à des partenaires étrangers. Le Comité a examiné les pratiques du Service en matière de partage d'information dans le contexte de plusieurs études antérieures, mais il a décidé de mener son premier examen poussé des échanges d'information du SCRS avec les proches partenaires alliés.

Méthode

À partir de l'une des enquêtes antiterroristes du Service, le Comité a choisi d'en examiner les échanges d'information avec quatre organismes alliés, comme objet premier de son examen détaillé. Celui-ci couvrait la période du 1er juin au 31 décembre 2003, mais par souci de minutie le CSARS a examiné certains documents hors de cette

13. Audience publique de la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar, transcription (22 juin 2004) p. 278, lignes 6-9.

période. Il a scruté tous les documents pertinents relatifs à l'enquête, en versions électronique et imprimée, afin de déterminer si ces échanges au sujet de menaces à la sécurité du Canada étaient conformes à l'entente conclue avec chacun des quatre organismes ainsi qu'à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le CSARS s'est penché sur :

- la portée de l'entente conclue avec chaque organisme étranger;
- le consentement ou l'autorisation nécessaire pour communiquer cette information;
- les conditions spéciales ou restrictions imposées à l'égard de l'utilisation de cette information;
- la nature de l'information partagée.

Constatations

Dans le contexte de l'enquête examinée, le CSARS a constaté que les échanges d'information du Service avec les services alliés étaient conformes à l'entente conclue avec chacun d'eux ainsi qu'à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Le Comité a aussi constaté que le Service avait fait preuve de diligence raisonnable en échangeant des informations au sujet des cibles d'enquête.

Dans le contexte de l'enquête examinée, le CSARS a constaté que les échanges d'information du Service avec les services alliés étaient conformes à l'entente conclue avec chacun d'eux ainsi qu'à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le SCRS a obtenu l'approbation requise avant de communiquer les informations aux organismes alliés choisis, mais le CSARS lui a recommandé de modifier sa politique opérationnelle afin d'indiquer clairement quel niveau de gestion doit rendre compte des communications aux organismes étrangers. Cependant, le Service s'est dit d'avis que l'obligation redditionnelle dernière était clairement indiquée dans sa politique.

Le CSARS a recommandé que le SCRS modifie la politique opérationnelle afin d'indiquer clairement quel niveau de gestion doit rendre compte des communications aux organismes étrangers.

Dans cette étude, le CSARS a aussi examiné la place qui avait été faite aux droits de la personne dans le contexte des ententes conclues avec des organismes étrangers.

Lorsque le SCRS amorce le processus menant à une nouvelle entente avec un organisme étranger, il informe Affaires étrangères Canada et le ministre de la Sécurité publique et de la Protection civile qu'il « scrutera de près la teneur des renseignements fournis à un organisme étranger ou reçus de celui-ci afin d'*assurer* [les italiques sont de nous] qu'aucun de ces renseignements ne serve à commettre des actes susceptibles d'être considérés comme des violations des droits de la personne ou n'ait été obtenu par suite de tels actes ».

Le CSARS a noté deux questions découlant de cette déclaration.

Premièrement, l'emploi du terme « assurer » implique que le SCRS certifie que l'information partagée ne donne pas lieu à des actes susceptibles d'être considérés comme des violations de droits de la personne, ni ne découle de tels actes. **Le Comité a cependant conclu que le SCRS n'était pas en mesure de fournir cette assurance absolue.** Comme M. Elcock l'a affirmé devant la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar, le SCRS n'écarterait pas nécessairement des informations qui pourraient découler de violations de droits de la personne. Il a expliqué que « [nous du SCRS,] nous sommes là pour recueillir l'information … [susceptible] de révéler une menace envers la sécurité du Canada, et nous recherchons l'information de toute source pouvant nous renseigner sur les menaces envers la sécurité du Canada[14] ».

Le CSARS a constaté que l'assurance fournie au Ministre par le SCRS pourrait être mal interprétée, car celui-ci est rarement en mesure de déterminer l'usage qui est fait de l'information transmise à un organisme étranger ou la manière dont celle qu'il reçoit a été obtenue.

Deuxièmement, même si le SCRS est prudent lorsqu'il partage de l'information avec des organismes étrangers, il ne peut déterminer dans tous les cas l'usage que ceux-ci en font. De même, il est rarement en mesure de savoir comment une information reçue d'un organisme étranger a été obtenue. Comme M. Elcock l'a affirmé devant la Commission O'Connor, pour ce qui est des renseignements qui peuvent avoir été obtenus par la torture, « en réalité, dans la plupart des cas, nous ignorons que les renseignements sont le résultat de la torture. Nous pouvons nous douter que les renseignements ont été obtenus par la torture, mais dans la plupart des cas, nous ne pouvons aller plus loin que les soupçons[15] ».

14. Audience publique de la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar, transcription (21 juin 2004) p. 162, lignes 15-19.
15. Audience publique de la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar, transcription (21 juin 2004) p. 141, lignes 5-9.

En réponse à cette étude, le Service a pris pour position que toute sa correspondance avec la ministre de SPPC reflète un suivi constant de la situation. À son avis, il informe la Ministre que les échanges d'information avec un organisme allié correspondent au degré de confiance qui s'établit après un certain temps et reflète le climat qui règne dans le pays en cause sur le plan politique et sur celui des droits de la personne.

Le CSARS admet que le SCRS doit compter sur l'information reçue de ses partenaires étrangers pour remplir son mandat et que l'échange d'information entre services de renseignement de sécurité est un outil d'enquête essentiel. Cependant, il a constaté que l'assurance fournie au Ministre par le SCRS pourrait être mal interprétée, car celui-ci est rarement en mesure de déterminer l'usage qui est fait de l'information transmise à un organisme étranger ou la manière dont celle qu'il reçoit a été obtenue.

Le CSARS a recommandé que le SCRS revoie le contenu des lettres adressées à Affaires étrangères Canada et à la ministre de SPPC pour éviter de donner l'impression qu'il peut garantir que l'information fournie à un organisme étranger ou reçue de lui n'a pas servi à commettre des actes susceptibles d'être considérés comme des violations des droits de la personne et n'a pas, non plus, été obtenue par suite de tels actes.

Étude d'une enquête de contre-espionnage

Rapport nº 2004-06

Contexte

Dans cette étude, le CSARS a examiné une enquête menée par le SCRS sur un service de renseignement étranger.

Méthode

L'examen de cette enquête de contre-espionnage par le CSARS a porté sur la période du 1er janvier au 31 décembre 2003. L'objectif était d'évaluer la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles et à toutes les politiques opérationnelles pertinentes.

Le CSARS a examiné les documents, versions papier et électronique, qui avaient trait aux activités d'ordre opérationnel suivantes du SCRS :

- ciblage d'individus soupçonnés d'exercer des activités constituant des menaces, et processus d'autorisation d'enquête;
- demande de mandat à la Cour fédérale;

- exercice des pouvoirs conférés par mandat contre les cibles autorisées;
- direction de sources humaines contre les cibles autorisées;
- conseils choisis aux ministères.

Comme dans toutes ses études, le CSARS a cherché à répondre à trois questions principales :

- Le SCRS avait-il des motifs raisonnables de soupçonner l'existence d'une menace à l'égard de la sécurité du Canada?
- Le niveau de l'autorisation d'enquête était-il proportionnel à la menace?
- Le Service a-t-il recueilli uniquement des informations strictement nécessaires à son enquête?

Constatations

Dans l'ensemble, l'enquête de contre-espionnage était conforme à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle au cours de la période à l'étude. Le CSARS a constaté que le SCRS avait des motifs raisonnables de soupçonner les cibles d'enquête autorisées de présenter une menace pour la sécurité du Canada. Il a également constaté que le degré d'intrusion des méthodes employées était proportionnel à la menace présumée que constituaient ces cibles. Les enquêteurs du SCRS ont recueilli uniquement des informations strictement nécessaires à l'enquête. Ils ont aussi agi d'une manière irréprochable et conforme à la loi dans leur recours aux sources humaines.

Le CSARS a constaté que le SCRS avait des motifs raisonnables de soupçonner les cibles d'enquête autorisées de présenter une menace pour la sécurité du Canada.

Le CSARS a constaté que la description des activités constituant des menaces, faite par le Service dans l'affidavit appuyant la demande de mandat, traduisait fidèlement l'information que celui-ci avait en sa possession. Le SCRS s'était conformé à toutes les politiques opérationnelles pertinentes pour la demande de mandat et aux conditions imposées par la Cour fédérale une fois sa demande approuvée. Le CSARS a aussi constaté que le Service avait respecté les conditions imposées dans le mandat par la Cour fédérale pour l'exercice des pouvoirs conférés dans ce document et pour la conduite d'opérations spéciales.

Le Comité a cependant observé que la portée du mandat était trop ambitieuse. Deux régions du SCRS ont mentionné que le manque de ressources humaines avait entravé leur capacité à analyser certains renseignements recueillis. Le CSARS a aussi noté

que le Service avait instauré une nouvelle méthode de collecte d'information au cours de la période à l'étude. Cette méthode sera examinée au cours de prochaines études.

Tout au long de l'étude, le Comité a porté une attention particulière à l'enquête du Service sur les activités d'ingérence. Pour en assurer la conformité à la *Loi sur le SCRS*, celui-ci avait pris soin d'élaborer des lignes directrices strictes pour régir ce volet de son enquête. Cependant, le CSARS a constaté que les politiques opérationnelles du Service visant ces types de situations étaient incomplètes. Aussi a-t-il recommandé que :

> **Le SCRS revoie et modifie, au besoin, ses politiques opérationnelles relatives à des institutions particulières pour assurer qu'elles couvrent tous les aspects d'un processus donné.**

Le Comité a porté une attention particulière à l'enquête du Service sur les activités d'ingérence.

Il est également à noter que, même si le Comité a constaté que le Service avait agi selon les règles en conseillant les représentants du gouvernement du Canada au sujet des activités du service de renseignement étranger, il estime néanmoins que le SCRS a été trop prudent en décidant de ne pas partager des informations avec un ministère fédéral. Le Service s'est dit en désaccord avec cette constatation et il estime que, compte tenu du caractère délicat de l'enquête, il avait adopté une approche judicieuse dans la diffusion de toute information.

Financement du terrorisme au Canada

Rapport nº 2004-10

Contexte

Depuis le 11 septembre 2001, la communauté internationale a intensifié ses efforts pour enrayer le financement du terrorisme. En décembre 2001, le Conseil de sécurité des Nations Unies a adopté la résolution 1373, invitant les États membres à bloquer les avoirs de ceux qui commettent ou facilitent des actes terroristes et à adopter des mesures pour prévenir et supprimer le financement du terrorisme. En réaction, le gouvernement du Canada a adopté le *Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme (RARNUIT)* et la *Loi antiterroriste*.

Le SCRS examine depuis toujours le financement du terrorisme à la lumière de ses enquêtes antiterroristes, mais la concertation des efforts à l'échelle internationale depuis le 11 septembre 2001 a obligé à acquérir un niveau de compétence spécialisé. En 2002, le SCRS a créé la Section du financement du terrorisme, à la Direction de l'antiterrorisme,

afin de dépister les structures financières qui soutiennent des organisations terroristes. Cette année-là, dans ses Exigences nationales en matière de renseignement de sécurité, le Ministre a, pour la première fois, ordonné expressément au SCRS de faire enquête sur la menace que constitue le financement du terrorisme et de conseiller le gouvernement du Canada à ce sujet.

Méthode

L'objectif de cette étude était d'examiner l'enquête du SCRS sur le financement du terrorisme au Canada et d'en faire une étude approfondie. Le Comité a choisi la cible d'une enquête contextuelle et cinq cibles particulières. Dans chaque cas, il a évalué la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle en examinant les activités d'ordre opérationnel suivantes :

- les décisions de ciblage;
- les activités en matière d'enquête et les rapports opérationnels;
- la coopération et les échanges d'information avec des organismes canadiens;
- la coopération et les échanges d'information avec des organismes étrangers.

La période considérée par le Comité était du 1er janvier 2003 au 31 juillet 2004. Cependant, pour être sûr d'aller au fond des choses, le CSARS a aussi examiné certains documents débordant cette période.

Constatations

Le Comité a conclu que le Service avait des motifs raisonnables de soupçonner les activités des individus et groupes ciblés de présenter une menace pour la sécurité du Canada. Le niveau et le degré d'intrusion de l'enquête du SCRS étaient proportionnels à la menace présumée, et celui-ci a recueilli uniquement des informations nécessaires à l'exécution de son mandat. Ses activités étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le CSARS a aussi constaté que le Service avait respecté en tous points les instructions ministérielles et la politique opérationnelle en ce qui touche les demandes d'autorisation d'enquête et de renouvellement. Les déclarations faites dans les demandes étaient appuyées par les rapports opérationnels du SCRS.

Enfin, le CSARS est satisfait du degré et de la nature de la coopération du Service avec ses partenaires canadiens et étrangers. Les échanges d'information avec eux étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Mise en œuvre du RARNULT

Au cours de cette étude, le Comité a appris que la mise en œuvre du *RARNULT* avait obligé le SCRS à assumer de nouvelles responsabilités quant à l'inscription des entités terroristes. Il n'a pas entrepris d'examen approfondi de la participation du Service à l'inscription d'entités en vertu du *RARNULT*, car cela débordait le champ de son étude. Cependant, le CSARS a noté que la participation du SCRS à ce processus avait soulevé d'importantes questions juridiques, apparentées à celles qu'il avait relevées dans l'étude du processus d'inscription des entités terroristes.

Devant les craintes du Comité face au processus d'inscription du *RARNULT*, le Service a affirmé qu'il recueillait et analysait uniquement des informations de sources ouvertes. Il est en désaccord avec l'idée que la collecte et la conservation d'informations publiques constituent un élargissement de son mandat.

Les critères d'inscription en vertu du *RARNULT* sont énoncés à l'article 2 de la législation où l'on peut lire qu'une personne ou un groupe peut être inscrit s'il y a des motifs raisonnables de croire que cette entité : *a*) s'est livrée ou a tenté de se livrer à une activité terroriste, ou a participé à son exercice ou l'a facilitée; *b*) est contrôlée directement ou non par une personne visée à l'alinéa *a*); ou *c*) agit au nom d'une personne visée à l'alinéa *a*), ou sous sa direction ou en collaboration avec elle.

Les entités peuvent être inscrites suivant deux modalités. Premièrement, elles peuvent faire l'objet d'une résolution du Conseil de sécurité de l'ONU, auquel cas leurs noms sont retenus d'office à titre d'entités inscrites en vertu du *Règlement d'application des résolutions des Nations Unies sur l'Afghanistan*. Deuxièmement, sur la recommandation du ministre des Affaires étrangères, le gouverneur en conseil peut décider de porter une entité sur la liste prévue au *RARNULT*. En pareil cas, Affaires étrangères Canada convoque une réunion interministérielle pour discuter de l'inscription proposée. Si le SCRS a des renseignements de sécurité au sujet de l'intéressée, il prépare pour son directeur une évaluation indiquant s'il a des motifs raisonnables d'en appuyer l'inscription. Cette évaluation est fournie à Affaires étrangères qui peut s'en servir, de même que des observations de nombreux autres ministères et organismes fédéraux, pour appuyer sa recommandation au gouverneur en conseil.

Le Service a dit au Comité qu'il prend part à l'inscription d'entités selon le *RARNULT* en vertu de l'article 12 de la *Loi sur le SCRS*, qui limite les activités de collecte du Service aux *menaces envers la sécurité du Canada*. Cependant, le CSARS a noté que la participation du SCRS au processus d'inscription l'oblige à déterminer si une entité

répond à la définition de *personne inscrite* en vertu du *RARNUIT*, qui ne contient pas de restriction géographique semblable. En conséquence, tout comme dans l'étude du CSARS sur le processus d'inscription des entités terroristes, il est possible que le Service soit tenu de recueillir et d'analyser des informations concernant une entité qui répond à la définition de *personne ou groupe inscrit* en vertu du *RARNUIT* mais qui ne présente pas une *menace envers la sécurité du Canada*. Le CSARS a relevé l'existence de ce problème en étudiant des rapports opérationnels.

Devant les craintes du Comité face au processus d'inscription du *RARNUIT*, le Service a affirmé qu'il recueillait et analysait uniquement des informations de sources ouvertes. Il est en désaccord avec l'idée que la collecte et la conservation d'informations publiques constituent un élargissement de son mandat. De plus, le CSARS a noté que le *RARNUIT* n'enjoint pas expressément au SCRS de prendre part au processus d'inscription; en outre, le ministre de la Sécurité publique et de la Protection civile n'a donné à cet égard aucune instruction particulière au SCRS. En effet, dans les Exigences nationales en matière de renseignement de sécurité 2003-2004, on ne fait que mentionner le processus d'inscription prévu dans le *Code criminel*, demandant au Service de poursuivre ses recherches et analyses pour appuyer l'inscription des entités terroristes en vertu de la *Loi antiterroriste*.

Le CSARS poursuivra l'étude de cette question. Comme toujours, il continuera à examiner les implications des nouvelles mesures législatives sur les activités d'ordre opérationnel du Service. Cette étude n'a donné lieu à aucune recommandation.

Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité

Rapport nº 2004-01

Contexte

Les bureaux de liaison-sécurité sont situés en des endroits stratégiques à l'étranger afin de combler les besoins du Service le plus efficacement possible. La Direction de la liaison avec l'étranger et des visites (LEV) du SCRS, qui supervise ces bureaux, fonde ses opérations sur le principe de la réciprocité. Le Service doit être prêt à fournir des informations aux services étrangers de renseignement de sécurité s'il veut en recevoir en retour. Les activités et échanges de cette nature sont généralement traités par ses bureaux de liaison-sécurité. Les emplacements de ces bureaux sont classifiés, mis à part ceux de Paris, Washington et Londres.

Sur les directives de la Direction de la LEV, les agents de liaison-sécurité (ALS) :

- assurent la liaison courante avec les services étrangers de renseignement de sécurité;
- fournissent des services de filtrage de sécurité à l'appui du programme d'immigration;
- supervisent l'échange de renseignements de sécurité avec les organismes approuvés;
- conseillent les cadres supérieurs de la mission ou de l'ambassade canadienne;
- rendent compte au directeur général de LEV, aux gestionnaires des opérations à l'Administration centrale et au chef de mission de la zone relevant de chaque ALS.

Le CSARS examine régulièrement les bureaux de liaison-sécurité du Service, suivant le sous-alinéa 38*a*)(iii) de la *Loi sur le SCRS*. Cette année, il en a choisi un qui était ouvert depuis peu.

Méthode

Dans son examen, le Comité a cherché à déterminer si les échanges d'information de ce bureau de liaison-sécurité avec des organismes étrangers respectaient la portée des ententes de liaison existantes, approuvées par le gouvernement. Il en a aussi évalué les opérations par rapport à la *Loi sur le SCRS* et aux instructions ministérielles ainsi qu'aux politiques et procédures opérationnelles du Service.

Le Comité a mené cette étude en examinant des documents à l'Administration centrale du SCRS et en visitant le bureau de liaison-sécurité. Pour se mettre en contexte, il en a aussi examiné les opérations et les a évaluées par rapport aux questions qui se posent lors de l'examen suivi des ententes du SCRS avec des organismes étrangers, en vertu de la loi. De plus, dans son rapport, le CSARS a tenu compte des tendances observées dans ses études des cinq dernières années sur les ALS.

L'étude a gravité autour de deux questions principales : la charge de travail en matière de filtrage de sécurité et la sécurité dans ce bureau.

Constatations

a) Conformité et efficacité

Au cours de la période à l'étude, ce bureau du Service n'a pas eu suffisamment d'échanges avec des organismes étrangers pour que le Comité puisse déterminer de façon décisive s'ils étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle du Service. L'examen des échanges par le CSARS laisse toutefois entrevoir que le SCRS a mené ses nouveaux rapports de liaison avec la prudence requise.

Cependant, le manque de documents du SCRS qui aient été mis à jour, pour évaluer les rapports de liaison de ce bureau, a suscité certaines préoccupations au Comité. En dépit des directives écrites concernant l'élaboration, la présentation et la mise à jour de tels documents, le SCRS n'a pas de politique officielle à cet égard. Compte tenu de la situation observée dans ce bureau et du nombre croissant des échanges du Service avec des organismes étrangers, le CSARS a formulé la recommandation suivante :

> **Le Comité a recommandé que le Service instaure des politiques pour l'élaboration, la mise à jour et la présentation annuelle des documents qui servent à évaluer les échanges avec des organismes étrangers.**

Le Comité a aussi recommandé que les directives écrites de la Direction de la LEV, concernant les procédures à suivre dans les bureaux de liaison-sécurité, soient mises à jour afin de refléter les pratiques réelles du Service.

b) Filtrage de sécurité

L'une des fonctions des ALS est d'aider Citoyenneté et Immigration Canada et l'Agence des services frontaliers du Canada à filtrer les immigrants éventuels au pays. Si les employés de l'un ou l'autre de ces organismes, chargés du filtrage à l'immigration dans un bureau de liaison-sécurité, nourrissent des craintes au sujet de la sécurité, ils peuvent soumettre l'affaire à l'ALS qui enquête à ce sujet.

Le manque de documents du SCRS qui aient été mis à jour, pour évaluer les rapports de liaison de ce bureau, a suscité certaines préoccupations au Comité.

Le Comité note que la charge de travail des ALS en matière de filtrage de sécurité a été qualifiée de problème lors de chacune de ses études des cinq dernières années sur les ALS. Dans son tout dernier rapport, il s'est à nouveau dit préoccupé par leur charge de travail sur ce plan et il a suggéré au Service d'adopter des repères numériques pour cerner et régler les problèmes en ce domaine.

c) La sécurité dans ce bureau

Le CSARS a scruté le contexte de fonctionnement du bureau. Il a conclu que l'action des ALS y était conforme aux procédures de sécurité du SCRS.

Le rôle des agents de liaison-sécurité du SCRS

Voici les fonctions qu'exercent les agents de liaison-sécurité du SCRS au nom de celui-ci lorsqu'ils sont affectés dans des bureaux à l'étranger :

- entretenir et élargir les voies de communication avec les organismes étrangers avec lesquels le Service a des ententes approuvées;
- exécuter les activités de filtrage de sécurité propres à appuyer le Programme fédéral de filtrage des demandes d'immigration;
- signaler à l'Administration centrale du SCRS toute question liée aux impératifs du Canada en matière de sécurité nationale;
- effectuer les vérifications de fiabilité particulières demandées par l'agent de sécurité du bureau.

Toute aide opérationnelle apportée par le Service ou toute activité d'enquête qu'il mène à l'extérieur du pays, à l'égard de menaces envers la sécurité du Canada (article 2 de la *Loi sur le SCRS*), est distincte des fonctions et responsabilités des agents de liaison-sécurité.

Examen des ententes avec des organismes étrangers

Contexte

En vertu du paragraphe 17(1) de la *Loi sur le SCRS*, le Service peut conclure une entente avec le gouvernement d'un État étranger, ou avec une organisation internationale d'États (ou avec ses institutions), dans le but d'exercer ses fonctions. Les instructions ministérielles et la politique opérationnelle du SCRS énoncent les principes régissant la conclusion et la gestion de ces ententes, mais c'est l'entente même, conclue avec un organisme étranger, qui détermine la nature et l'ampleur de la coopération et les échanges du Service avec lui. Elle précise les types particuliers de partage d'information qui sont autorisés.

En vertu du sous-alinéa 38*a*)(iii), le Comité est tenu d'examiner toutes ces ententes. À cet égard, il se penche à la fois sur l'établissement et sur l'amélioration des ententes conclues entre le SCRS et des services de renseignement étrangers.

Tel que mentionné dans de précédents rapports, un recueil d'instructions ministérielles est entré en vigueur le 1er mars 2001. Le directeur du SCRS a ainsi une plus grande latitude pour gérer les activités du Service. Par exemple, il peut approuver l'élargissement d'une entente conclue avec un organisme étranger (et déjà approuvée à la fois par le

ministre de la Sécurité publique et de la Protection civile et par son homologue des Affaires étrangères). Le SCRS n'est pas tenu de consulter le ministère des Affaires étrangères ni de demander l'autorisation du Ministre pour le faire. En conséquence, le pouvoir discrétionnaire du directeur est plus vaste dans ce domaine d'activité du Service.

Études effectuées en 2004-2005

Au cours de 2004-2005, le Comité a réalisé une étude approfondie du processus d'élargissement d'ententes, sa première depuis l'entrée en vigueur du recueil d'instructions ministérielles. Il s'est concentré sur les dix ententes élargies entre le 1er avril 2002 et le 31 mars 2003 afin de déterminer si elles étaient conformes aux instructions ministérielles et à la politique opérationnelle. Il y a amélioration ou élargissement d'une entente existante lorsque le Service la modifie. Cela définit la teneur et l'ampleur des échanges autorisés.

Le Comité a réalisé une étude approfondie du processus d'élargissement d'ententes, sa première depuis l'entrée en vigueur du recueil d'instructions ministérielles.

Pour chaque entente avec un organisme étranger, le personnel du CSARS a examiné :

- les motifs de la demande d'élargissement;
- les impératifs du Canada en matière de sécurité nationale;
- la demande d'élargissement de l'entente;
- l'autorisation à l'élargir;
- l'évaluation de l'organisme par le Service (c.-à-d. la façon dont il respecte la règle de l'information fournie par des tiers, sa fiabilité, les questions liées aux droits de la personne, les inquiétudes au sujet de la stabilité intérieure, etc.).

Le personnel du CSARS a étudié :

- tous les documents concernant l'établissement de l'entente, selon l'article 17 de la *Loi sur le SCRS* et les instructions du Ministre;
- tous les documents concernant l'élargissement de l'entente;
- le dossier de la coopération avec l'organisme;
- l'évaluation la plus récente de cet organisme;
- le tout dernier profil du bureau établi par l'agent de liaison-sécurité;
- toute autre information ayant trait à l'entente et à son amélioration.

Constatations

Le CSARS a constaté que le SCRS s'était conformé aux conditions énoncées dans les instructions ministérielles et dans la politique opérationnelle à l'égard de l'élargissement des dix ententes existantes, conclues avec des organismes étrangers.

Au sujet des autorisations d'élargissement, le Comité a noté que le Service n'avait pas de politique opérationnelle quant au type d'informations à inclure dans la demande présentée au directeur. Il a aussi noté que les évaluations des organismes avec lesquels le SCRS a des ententes n'étaient pas toujours présentées chaque année, tel que prescrit dans le Manuel des procédures pour les postes de la Liaison avec l'étranger, et qu'elles étaient périmées depuis un bon moment dans certains cas. La question des évaluations d'organismes a fait l'objet d'une recommandation dans l'étude nº 2004-01.

Ce qui préoccupe davantage le Comité, cependant, c'est que l'évaluation d'un organisme ne contenait pas d'analyse satisfaisante des problèmes possibles liés aux droits de la personne. Comme l'élargissement suppose une coopération accrue avec un organisme étranger, le CSARS estime qu'une réévaluation complète de ces organismes devrait être

Orientations générales concernant les ententes avec des organismes étrangers

La *Loi sur le SCRS* confère au Service le pouvoir de conclure des ententes avec les organismes de gouvernements étrangers et avec des organisations internationales. Ces ententes doivent être approuvées par le ministre de la Sécurité publique et de la Protection civile, après consultation du ministre des Affaires étrangères. Les instructions ministérielles dictent les procédures et les conditions à respecter pour conclure une nouvelle entente ou élargir la portée d'une entente existante. De plus, elles habilitent le directeur du SCRS à gérer ces ententes suivant les conditions imposées par le Ministre.

Selon les instructions ministérielles, les ententes doivent respecter les critères suivants :

- il faut conclure les ententes qui s'imposent pour assurer la sécurité du Canada;
- celles-ci doivent demeurer compatibles avec les objectifs de la politique étrangère canadienne à l'égard du pays ou de l'organisation internationale signataire;
- les ententes doivent respecter les lois applicables du Canada;
- il faut évaluer le bilan du pays ou de l'organisme en cause, en matière de respect des droits de la personne, et tenir compte de cette évaluation dans toute décision de nouer des rapports de coopération.

La nature des relations entre le SCRS et un organisme étranger est établie lorsque le Service conclut une entente qui l'autorise à échanger de l'information ou à coopérer avec lui dans des domaines particuliers. Le SCRS peut aussi élargir la portée des ententes pour englober des échanges d'information particuliers ou pour les limiter à certaines sphères.

requise au moment de l'élargissement pour assurer que les ententes visées demeurent l'objet d'un examen rigoureux, notamment en ce qui touche les droits de la personne.

L'évaluation d'un organisme ne contenait pas d'analyse satisfaisante des problèmes possibles liés aux droits de la personne.

Le SCRS est d'avis que, lorsqu'on envisage d'élargir une entente, la Direction de la LEV fournit au directeur l'information voulue pour qu'il puisse prendre une décision éclairée, à savoir s'il doit ou non y avoir élargissement. Selon le Service, l'absence d'évaluation à jour de l'organisme intéressé ne signifie pas qu'une étude de l'entente n'a pas été préparée pour le directeur.

B. Enquêtes sur les plaintes

Outre sa fonction de surveillance, le Comité a charge d'enquêter sur les plaintes du public au sujet du SCRS. Quatre types de plaintes peuvent lui être adressées pour qu'il fasse enquête :

- les plaintes de particuliers « contre des activités du Service » (article 41);
- celles concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État (article 42);
- les plaintes dont la Commission canadienne des droits de la personne saisit le CSARS;
- les rapports du Ministre à l'égard de la *Loi sur la citoyenneté*.

S'il y a lieu, le Comité fait enquête sur les plaintes dans le cadre d'audiences quasi judiciaires que préside l'un de ses membres.

Dans ses enquêtes sur les plaintes, le CSARS détermine si le Service a mené ses activités conformément à la *Loi sur le SCRS*, aux instructions ministérielles et à sa politique.

À la suite d'une enquête visée à l'article 41, le Comité est tenu, en vertu de la *Loi sur le SCRS*, de présenter au Ministre et au directeur du Service un rapport énonçant les conclusions de son enquête et les recommandations qu'il juge indiquées. La *Loi* lui enjoint également de communiquer au plaignant ses conclusions et, s'il le juge à propos, d'y joindre les recommandations faites au Ministre et au directeur.

À la suite d'une enquête visée à l'article 42, le CSARS présente au Ministre, au directeur du SCRS, à l'administrateur général de l'organisme gouvernemental intéressé et au plaignant un rapport contenant les recommandations qu'il juge indiquées et les conclusions qu'il estime à propos de communiquer à celui-ci.

Le tableau 1 montre l'état de toutes les plaintes qui ont été présentées au CSARS au cours des trois derniers exercices, y compris celles qui lui ont été adressées à tort, qui ont été jugées hors de sa compétence ou qui ont fait l'objet d'une enquête et d'un règlement sans audience (examen administratif).

Tableau 1
Règlement des plaintes*

Description	2002-2003	2003-2004	2004-2005
Reportées de l'exercice précédent	17	17	16
Nouvelles	48	30	30
Total	**65**	**47**	**46**
Réglées	48	31	28
Reportées à l'exercice suivant	17	16	18

* Le tableau fait état de l'ensemble des plaintes reçues par le Comité. Cependant, leur étude n'a pas forcément débouché dans chaque cas sur une enquête du CSARS. Certaines plaintes ont été renvoyées aux organismes gouvernementaux compétents ou déclarées dès le départ comme débordant la compétence du Comité, et d'autres ont été retirées par leur auteur.

Rapports de décisions : résumés des plaintes

Voici les résumés des trois décisions que le CSARS a rendues au cours de la période à l'étude à l'égard de plaintes qui lui avaient été présentées.

RAPPORT : RENVOI D'UNE PLAINTE EN MATIÈRE DE DROITS DE LA PERSONNE

Le Comité a fait rapport d'une décision concernant une plainte dont la Commission canadienne des droits de la personne l'avait saisi en vertu de l'article 45 de la *Loi canadienne sur les droits de la personne*.

Le plaignant, un ex-employé du Service, s'est dit victime de discrimination de la part du SCRS, en violation de cette loi. En particulier, il s'est plaint de ce que le Service avait omis de moduler ses heures de travail et de l'autoriser à s'absenter du travail, manquant par là à son obligation de prendre des mesures d'adaptation qui tiennent compte des incapacités physiques et mentales du plaignant.

Le plaignant travaillait un nombre limité d'heures par semaine en raison d'incapacités. Le Service avait besoin que les fonctions de son poste soient remplies à plein temps : leur exercice à temps partiel lui aurait occasionné des difficultés excessives. Le Comité a conclu que le SCRS n'avait ni manqué à son obligation de prendre des mesures d'adaptation à l'égard du plaignant ni fait des distinctions injustes à son égard pour des motifs condamnés dans la *Loi canadienne sur les droits de la personne*. Cependant, il a noté que le Service aurait pu être plus délicat dans la manière dont il avait fait part de sa décision indiquant qu'il ne pouvait accepter que le plaignant travaille à temps partiel.

De plus, le Comité a déterminé que, compte tenu des craintes liées à la sécurité nationale entourant l'enquête sur la plainte, ni la Commission canadienne des droits de la personne ni le Tribunal canadien des droits de la personne ne pouvaient effectuer d'enquête ou d'audience significative à l'égard de la plainte.

En conséquence, le Comité a recommandé que la Commission canadienne des droits de la personne rejette la plainte.

Le Comité a conclu que le SCRS n'avait ni manqué à son obligation de prendre des mesures d'adaptation à l'égard du plaignant ni fait des distinctions injustes à son égard pour des motifs condamnés dans la *Loi canadienne sur les droits de la personne*. Cependant, il a noté que le Service aurait pu être plus délicat dans la manière dont il avait fait part de sa décision indiquant qu'il ne pouvait accepter que le plaignant travaille à temps partiel.

RAPPORT : ARTICLE 41 (« ACTIVITÉS DU SERVICE »)

Le Comité a fait rapport d'une décision concernant une plainte en vertu de l'article 41 de la *Loi sur le SCRS*; selon cet article, toute personne peut porter plainte contre « des activités du Service ».

Le plaignant avait allégué qu'un employé du Service n'avait pas mené comme il fallait les entrevues de filtrage de sécurité à l'immigration qu'il avait subies. Après audience et examen de la preuve, le CSARS a conclu que le plaignant n'avait présenté aucun élément de preuve permettant de croire que les entrevues avaient été menées de façon incorrecte.

Le Comité a déterminé que, pour diverses raisons, dont le fait que la langue première du plaignant n'était ni le français ni l'anglais, il y aurait eu méprise ou confusion dans l'esprit de celui-ci au cours du processus de filtrage à l'immigration, en raison d'une lettre de Citoyenneté et Immigration Canada.

RAPPORT : ARTICLE 42 (REFUS D'UNE HABILITATION DE SÉCURITÉ)

Le CSARS a fait rapport d'une décision concernant une plainte, en vertu de l'article 42 de la *Loi sur le SCRS*, au sujet du refus d'une habilitation de sécurité.

La décision de l'administrateur général de refuser l'habilitation de sécurité était raisonnable et le CSARS a recommandé que la décision soit confirmée.

Le plaignant a fait une demande d'emploi auprès d'un organisme fédéral qui lui a refusé une cote de sécurité requise, sur la foi de renseignements reçus du SCRS. Il a contesté ce refus en présentant une plainte au CSARS.

Le plaignant voulait obtenir une cote de sécurité « Très secret ». Selon la Politique du gouvernement sur la sécurité, une telle cote ne peut être octroyée s'il y a des motifs raisonnables de douter de la loyauté du demandeur envers le Canada ou de sa fiabilité en ce qui concerne sa loyauté.

Le Comité a conclu à l'existence de motifs raisonnables de croire que le plaignant avait pu se livrer à des activités de collecte de renseignements au nom d'un État étranger, et qu'il semblait avoir entretenu des rapports réguliers avec des représentants étrangers qui auraient pu avoir participé à de telles activités. En conséquence, la décision de l'administrateur général de refuser l'habilitation de sécurité était raisonnable et le CSARS a recommandé que la décision soit confirmée.

Plaintes au sujet d'activités du SCRS en vertu de l'article 41

En vertu de l'article 41 de la *Loi sur le SCRS*, le Comité est tenu de faire enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour qu'il fasse enquête, deux conditions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;

2. le Comité doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi. Conformément au paragraphe 41(2) de la *Loi*, il ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs en vertu de la *Loi sur le SCRS* ou de la *Loi sur les relations de travail dans la fonction publique*.

Plaintes au sujet d'activités du SCRS en vertu de l'article 42

En ce qui a trait aux décisions d'administrateurs généraux de refuser une habilitation de sécurité, le Comité de surveillance est tenu, selon l'article 42 de la *Loi sur le SCRS*, d'enquêter sur les plaintes présentées par :

1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une promotion ou une mutation pour la même raison;

3. les personnes qui se voient refuser un contrat de fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Une plainte ressortissant à l'article 42 de la *Loi* doit être présentée dans les 30 jours du refus d'une habilitation de sécurité. Le CSARS peut prolonger cette période si on lui fait part de raisons valables.

Renvois en vertu de la *Loi canadienne sur les droits de la personne*

Selon le paragraphe 45(2) de la *Loi canadienne sur les droits de la personne*, si la Commission canadienne des droits de la personne reçoit un avis écrit d'un ministre fédéral l'informant que les actes visés dans une plainte mettent en cause la sécurité nationale, elle peut rejeter la plainte ou transmettre l'affaire au CSARS. Sur réception d'un tel renvoi, le Comité fait enquête et, après avoir consulté le directeur du Service selon l'article 55 de la *Loi sur le SCRS*, il fait rapport de ses constatations à la Commission, au ministre qui l'a saisi de la plainte et au plaignant.

C. Rapport au ministre de la Sécurité publique et de la Protection civile selon l'article 54

En vertu de l'article 54 de la *Loi sur le SCRS*, le CSARS peut faire rapport au ministre de la Sécurité publique et de la Protection civile sur toute question relative à l'exercice des fonctions du Service.

À l'automne 2003, le CSARS a déterminé que les événements auxquels Maher Arar avait été mêlé étaient suffisamment importants pour justifier un rapport spécial de cette nature. Les constatations détaillées du rapport ne peuvent être dévoilées étant donné que la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar (Commission O'Connor) poursuit son enquête à ce sujet, mais ce cas illustre l'épineux dilemme devant lequel le Comité se trouve souvent. En raison de l'obligation que lui confère la loi de protéger la sécurité nationale et de veiller aux préoccupations entourant les renseignements personnels, le CSARS a souvent du mal à faire saisir la rigueur ou la complexité de ses études, ou à fournir des détails susceptibles d'aider à faire voir le bien-fondé de ses constatations et recommandations.

Le CSARS a été critiqué injustement lorsque le gouvernement a publié une version lourdement expurgée de son rapport classifié, sans le consulter. Le Comité a affirmé publiquement qu'il n'aurait « aucune objection » à ce que la Commission O'Connor publie un résumé de ce rapport une fois qu'elle aurait terminé sa propre enquête.

Le Comité a amorcé son étude en vertu de l'article 54 plusieurs mois avant la création de la Commission d'enquête. Il a examiné tous les documents à sa disposition en vertu de la *Loi sur le SCRS*, et il a fait part de ses constatations à la Ministre en mai 2004. Le rapport entier a été communiqué à la Commission, mais le CSARS a été critiqué injustement lorsque le gouvernement a publié une version lourdement expurgée de son rapport classifié, sans le consulter. Le Comité a affirmé publiquement qu'il n'aurait « aucune objection » à ce que la Commission O'Connor publie un résumé de ce rapport une fois qu'elle aurait terminé sa propre enquête.

Comme on l'a vu plus haut, le Comité ne peut examiner que les activités du SCRS. Cependant, en faisant son étude, il a cerné un certain nombre de questions qui semblaient justifier un examen par la Commission d'enquête sur les actions des responsables canadiens dans l'affaire Maher Arar :

- le rôle d'autres ministères et organismes fédéraux dans l'extradition d'Arar en Jordanie par les autorités américaines;
- la détention ultérieure d'Arar et son interrogatoire en Syrie;
- la présence éventuelle de renseignements du SCRS dans les dossiers de la GRC qui ont été communiqués aux autorités américaines;
- la manière dont les États-Unis sont entrés en possession du bail de location d'Arar, daté de 1998.

Le CSARS a conclu que la Commission O'Connor souhaiterait peut-être aussi faire des observations au sujet des mécanismes de protection qui sont prévus pour les citoyens canadiens dans la nouvelle entente consulaire entre le Canada et les États-Unis, annoncée le 13 janvier 2004 par le ministre canadien des Affaires étrangères.

Section 2

Mécanismes redditionnels du SCRS

Mécanismes redditionnels du SCRS

A. Exigences en matière de rapports

Le directeur du SCRS est tenu de présenter au Ministre, au moins une fois l'an, un rapport sur les activités d'ordre opérationnel du Service conformément au paragraphe 33(1) de la *Loi sur le SCRS*. Ce rapport est ensuite remis à l'inspecteur général. Après l'avoir reçu, celui-ci doit faire parvenir au Ministre un certificat exposant dans quelle mesure il est satisfait du rapport et l'informer de toute activité non autorisée ou de toute action ayant donné lieu à un exercice abusif ou inutile de pouvoirs. Le Ministre doit alors faire transmettre au CSARS le rapport du directeur et le certificat de l'inspecteur général.

En vertu du sous-alinéa 38*a*)(i) de la *Loi sur le SCRS*, le Comité est tenu d'examiner le rapport du directeur et le certificat de l'inspecteur général. L'étude de ces deux documents lui a été utile pour déterminer les domaines sur lesquels il pourrait faire porter de futures recherches et études. Le CSARS se sert aussi de ces documents pour comparer les activités du SCRS, une année sur l'autre, et pour surveiller l'efficacité des programmes et secteurs existants et nouveaux.

Dans cette section de son rapport annuel, le CSARS traite du rapport du directeur et du certificat de l'inspecteur général et il fournit un résumé des autres rapports qui sont exigés du SCRS.

CERTIFICAT DE L'INSPECTEUR GÉNÉRAL POUR 2004

Le poste d'inspecteur général (IG) a été créé en 1984 en vertu de la *Loi sur le SCRS*. Son titulaire joue pour le Ministre le rôle de vérificateur interne en scrutant les opérations du Service. Il relève du sous-ministre de la Sécurité publique et de la Protection civile, fournissant un moyen indépendant d'assurer que le Service respecte la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle.

Le certificat remis en novembre 2004 était le premier de l'inspecteur général en poste, qui avait été nommée en décembre 2003. Le CSARS a noté qu'elle a adopté le même processus de validation que son prédécesseur, à savoir l'examen d'informations et de renseignements choisis que le Service recueille et conserve. Cela comprend les comptes rendus d'activités des directions et les rapports de renseignement « servant à établir des faits » sur lesquels ils s'appuient.

L'IG a aussi décidé d'examiner :

- un échantillon choisi de mandats, de cibles et de cas de gestion de sources humaines;
- un échantillon d'ententes du SCRS avec des organismes étrangers;
- l'assistance prêtée par le Service aux ministères des Affaires étrangères et de la Défense nationale pour la collecte, au Canada, de renseignements sur des personnes et des États étrangers;
- la participation du SCRS au Centre intégré d'évaluation de la sécurité nationale, au processus d'attestation de danger pour la sécurité et à une opération de contre-espionnage.

Dans le certificat, on peut lire que le directeur du SCRS a aussi signalé cinq incidents de non-conformité aux règles générales en matière opérationnelle en 2003-2004. L'IG s'est penchée sur chacun de ces incidents et a constaté que des mesures appropriées avaient été prises dans chaque cas.

Dans le certificat de cette année, l'inspecteur général a fait rapport à la Ministre qu'elle était « satisfaite autant que je puisse l'être » du rapport annuel du directeur sur les activités d'ordre opérationnel du Service. Elle a conclu que le Service avait fait montre d'un professionnalisme digne d'éloges dans l'exercice de ses fonctions.

RAPPORT OPÉRATIONNEL ANNUEL DU DIRECTEUR DU SCRS, 2003-2004

Comme on l'a vu plus haut, le directeur du SCRS prépare chaque année un rapport destiné au ministre de la Sécurité publique et de la Protection civile et exposant les activités d'ordre opérationnel du Service. Dans ce rapport, qui est transmis au CSARS pour étude, il expose les réalisations de son organisme et les défis que celui-ci a eu à relever au cours de la période précédente.

Dans son rapport annuel de 2003-2004, le directeur a noté que les ressources du SCRS avaient augmenté depuis les attentats du 11 septembre; de plus, il a fait état des difficultés particulières du Service à faire face aux exigences liées au contexte actuel de la menace. Il a aussi a noté que la plus grande difficulté est peut-être le caractère international et transnational des menaces pour la sécurité du Canada, ce qui a élargi le champ des opérations du SCRS. Le meilleur moyen de se renseigner sur les menaces issues de l'étranger consiste de plus en plus à aller chercher les informations sur place, là où elles prennent naissance, a-t-il ajouté. Le directeur a en outre souligné que le Service avait un besoin croissant d'opérations conjointes et devait s'efforcer de nouer des relations afin d'accroître sa capacité de liaison avec ses partenaires canadiens et ses alliés étrangers.

i. Antiterrorisme

Dans le rapport, on peut lire que les plus hautes priorités du Service demeurent la sécurité publique et la protection contre le risque d'attentats terroristes exécutés ou préparés au Canada. L'enquête antiterroriste prioritaire, sur l'extrémisme islamique sunnite, y est décrite. D'autres enquêtes antiterroristes en cours y sont résumées, y compris le lancement d'une nouvelle enquête sur le risque de violence liée à l'instabilité et à un conflit dans un certain pays. L'atténuation de la menace a amené le SCRS à clore une enquête particulière. Le directeur a aussi décrit les autorisations d'enquêter sur certaines organisations terroristes, surtout en ce qui a trait aux activités de financement et de soutien menées au Canada.

Les activités de la Section du financement du terrorisme, à la Direction de l'antiterrorisme, sont aussi résumées. Ce groupe fournit au gouvernement du Canada des renseignements sur la nature et l'importance des réseaux de financement du terrorisme au pays. Le 1er avril 2004, 24 organismes étaient inscrits par suite du processus d'inscription des entités terroristes.

ii. Lutte contre la prolifération

Le rapport du directeur décrit les enquêtes en cours, dont celles sur le terrorisme parrainé par l'État ainsi que sur l'ingérence et les activités d'espionnage de certains gouvernements étrangers. La Direction de la lutte contre la prolifération (DLP) était aussi chargée de la Section des opérations de lutte contre la prolifération, de la Section du renseignement étranger et du Centre intégré d'évaluation de la sécurité nationale, dont la réorganisation devait donner naissance au Centre intégré d'évaluation des menaces (CIEM), sous la direction du conseiller du premier ministre à la sécurité nationale.

La DLP du SCRS a enquêté sur la menace constante que présente la prolifération des armes de destruction massive. Le directeur a signalé que, compte tenu du caractère international de la menace, nombre des enquêtes du Service sur la lutte contre la prolifération ont exigé une coopération étroite avec les services de renseignement alliés.

iii. Centre d'évaluation des menaces

Le rapport expose aussi les activités du Centre d'évaluation des menaces de la DLP, dont relève, entre autres, la Sous-section des évaluations de la menace. Celle-ci est chargée d'analyser les menaces potentielles contre les intérêts canadiens au pays et à l'étranger et celles qui visent les intérêts étrangers et les personnes bénéficiant d'une protection internationale, au Canada ou de passage en territoire canadien. Le rapport fait état de l'introduction de niveaux de menace définis et de la création d'un groupe de travail au sein de la Sous-section à Ottawa.

Le directeur a signalé que la DLP avait travaillé en étroite collaboration avec Citoyenneté et Immigration Canada, l'Agence des services frontaliers du Canada et l'ancienne Agence des douanes et du revenu du Canada pour empêcher d'entrer au pays des individus susceptibles de faire peser une menace sur la sécurité nationale ou pour être tenue informée de ceux qui sont admis en territoire canadien.

Le rapport fournit aussi des détails sur les activités de la Direction pour appuyer les efforts en vue d'expulser deux individus du Canada et pour assurer un soutien juridique à l'égard de deux autres cas qui sont actuellement l'objet d'une évaluation du danger.

iv. Centre intégré d'évaluation de la sécurité nationale

Au cours de 2003-2004, le directeur du SCRS a aussi fait rapport à la Ministre sur les travaux du Centre intégré d'évaluation de la sécurité nationale (CIESN), devenu opérationnel en février 2003. Ce groupe réunissait des organismes fédéraux investis de responsabilités diverses en matière de sécurité nationale et des participants admis, et leur permettait de consulter, de partager, d'analyser et de diffuser des informations et des renseignements. Le CIESN a axé ses efforts sur des sujets particuliers d'intérêt immédiat et à court terme. Il a depuis fait place au Centre intégré d'évaluation des menaces (CIEM), sous l'orientation stratégique du conseiller du premier ministre à la sécurité nationale. La responsabilité fonctionnelle courante du CIEM incombe au directeur du SCRS.

v. Contre-espionnage

Le rapport souligne les travaux de la Direction du contre-espionnage (CE). Celle-ci enquête sur les activités de certains pays qui consacrent beaucoup d'efforts à la collecte clandestine de renseignements politiques, militaires et économiques et à l'ingérence dans les affaires de communautés d'expatriés au Canada. Le rapport fait état des activités de certains pays et en mentionne d'autres qui ont fait l'objet d'enquêtes du CE.

vi. Programme des sources humaines

Le rapport du directeur fournit aussi des détails sur le programme des sources humaines du Service, notamment son coût et le nombre de celles-ci. On y décrit en outre l'exercice de pouvoirs délégués, par le directeur, à l'égard de certaines activités des sources, de même que les cas où l'approbation du Ministre est requise dans des circonstances particulières.

vii. Autres points principaux

Le directeur a noté que la création de l'Agence des services frontaliers du Canada constitue l'un des faits nouveaux les plus importants du Programme de filtrage des demandes d'immigration pour la période à l'étude. Il souligne les activités des quatre éléments de la Direction du filtrage de sécurité qui englobent le filtrage à l'immigration.

Le SCRS fournit des évaluations de sécurité à l'ensemble des ministères fédéraux (sauf la GRC) et il a plusieurs programmes d'accès à des sites, un programme destiné aux gouvernements provinciaux et des accords réciproques avec des organismes étrangers. Le rapport expose des activités particulières concernant chacun de ces programmes.

Au cours de la période à l'étude, le SCRS a géré 16 protocoles d'entente avec des ministères et organismes fédéraux et d'autres avec huit provinces. Le directeur n'a signalé aucune question importante à l'égard de ces protocoles.

Le rapport décrit en outre les activités du Service dans le cadre des 247 ententes qui étaient conclues avec des organismes étrangers au 31 mars 2004, dont 13 nouvelles, et la fusion de 3 ententes existantes. Aussi à noter, le directeur a fait état des efforts que la Direction des services techniques et scientifiques déploie et des défis qu'il lui faut relever.

AGISSEMENTS ILLICITES DE LA PART DU SCRS

En vertu du paragraphe 20(2) de la *Loi sur le SCRS*, le directeur du Service doit faire rapport au Ministre s'il estime qu'un employé peut avoir commis un acte illicite dans l'exercice de ses fonctions. Le cas échéant, le Ministre doit alors transmettre ce rapport au procureur général du Canada et au Comité, accompagné de ses observations.

En 2004-2005, le Service n'a signalé aucun acte illicite au Ministre.

ENQUÊTES EN VERTU DE L'ALINÉA 2*d*)

Le Service est autorisé à recueillir, à analyser et à conserver les informations et renseignements concernant les activités dont on peut soupçonner qu'elles constituent une menace envers la sécurité du Canada. Selon l'alinéa *d*) de la définition de « menaces », à l'article 2 de la *Loi sur le SCRS*, ce terme englobe les activités qui visent à saper le régime de gouvernement au Canada par des actions cachées et illicites, ou dont le but est de détruire ou de renverser ce régime par la violence. Le ministre de la Sécurité publique et de la Protection civile doit autoriser les enquêtes du Service sur ces menaces. D'après celui-ci, aucune enquête semblable n'a été autorisée en 2004-2005 en vertu de cet alinéa.

COMMUNICATION D'INFORMATIONS POUR RAISONS D'INTÉRÊT PUBLIC OU NATIONAL

Le Service ne peut communiquer les informations qu'il obtient dans l'exercice de ses fonctions que s'il se conforme aux conditions particulières énoncées à l'article 19 de la *Loi sur le SCRS*. L'alinéa 19(2)*d*) de la *Loi* habilite le Ministre à autoriser la communication d'informations aux personnes désignées dans cet article si cela est dans l'intérêt public et si cet intérêt justifie une éventuelle violation de la vie privée.

Le Service a informé le CSARS qu'aucune communication semblable n'avait été autorisée en 2004-2005.

Communication d'informations par le SCRS

L'article 19 de la *Loi sur le SCRS* prévoit quatre situations où le Service peut fournir des informations obtenues dans l'exercice de ses fonctions. Selon les définitions du paragraphe 19(2), ces situations sont celles où l'on peut communiquer des informations :

a) pouvant servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, et cela, aux agents de la paix compétents pour mener l'enquête, au ministre de la Sécurité publique et de la Protection civile et au procureur général de la province concernée;

b) concernant la conduite des affaires étrangères du Canada, et cela, au ministre des Affaires étrangères;

c) concernant la défense du Canada, et cela, au ministre de la Défense nationale;

d) essentielles pour des raisons d'intérêt public, selon le Ministre, et cela, à un ministre ou à un fonctionnaire fédéral. Le directeur du SCRS doit signaler au CSARS toute communication faite pour des raisons d'intérêt public.

B. Cadre d'action et de gestion

EXIGENCES NATIONALES ANNUELLES EN MATIÈRE DE RENSEIGNEMENT DE SÉCURITÉ

Contexte

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le ministre de la Sécurité publique et de la Protection civile énonce chaque année des exigences nationales en matière de renseignement de sécurité afin de donner au Service les orientations générales à suivre dans l'exercice de ses responsabilités en matière de collecte, d'analyse et de conseil. Ces responsabilités sont exposées en détail dans la *Loi*.

Selon les Exigences nationales de 2004-2005, le Service doit continuer de maintenir une capacité d'alerte souple et combler les besoins changeants du Canada en matière de renseignement de sécurité en composant avec la gestion du risque. La Ministre note que cette approche permettra au SCRS d'axer ses ressources sur les menaces principales tout en restant capable de résoudre sans délai les problèmes nouveaux. Le Service a pour directive de se concentrer sur les besoins de renseignements de sécurité touchant la sécurité du Canada, selon l'article 2 de la *Loi sur le SCRS*.

Pour 2004-2005, la Ministre a enjoint au SCRS de donner suite aux priorités suivantes, conformes à son mandat :

- prendre des mesures pour éviter qu'un attentat terroriste soit commis au Canada ou découle d'activités qui y sont menées ou affecte des citoyens ou des avoirs canadiens à l'étranger;
- évaluer la possibilité d'attentats au moyen d'armes de destruction massive;
- fournir des conseils au sujet de la sécurité économique du Canada;
- protéger les renseignements confidentiels du gouvernement du Canada;
- prodiguer des conseils à l'égard des menaces contre les infrastructures essentielles.

Dans les Exigences nationales de 2004-2005, la Ministre note que le contexte actuel de la menace a de plus en plus un caractère international et transnational : il ne faut donc pas suspendre les efforts du renseignement à la frontière canadienne. En conséquence, il est enjoint au SCRS de puiser aux sources étrangères d'informations liées à la menace. Il lui est aussi enjoint d'appuyer l'établissement et le fonctionnement du Centre intégré d'évaluation des menaces (CIEM), dans le cadre de l'engagement du gouvernement du Canada à l'égard d'un meilleur partage de l'information, et d'assurer la diffusion rapide de ses évaluations. Le CIEM remplacera le Centre intégré d'évaluation de la sécurité nationale (CIESN) du SCRS.

Les Exigences nationales reconnaissent la volonté manifeste d'individus, de groupes et d'États de recourir à la violence pour atteindre des objectifs à caractère politique, religieux, idéologique ou territorial. La Ministre note que les cibles privilégiées englobent les endroits où la destruction et le nombre de victimes seraient les plus grands possible. On reconnaît en outre dans les Exigences nationales que le Canada a relevé son profil face aux actes terroristes, à l'égard de ceux qui les commettent ou les parrainent.

> La Ministre note que le contexte actuel de la menace a de plus en plus un caractère international et transnational : il ne faut donc pas suspendre les efforts du renseignement à la frontière canadienne.

Tel que mentionné précédemment, une bonne partie des groupes terroristes du monde sont représentés au Canada. La Ministre note que ces groupes exercent des activités comme la collecte de fonds, le lobbying, la fraude sur les documents, la préparation et l'exécution d'actes terroristes, la manipulation de communautés d'émigrés, le soutien du transit en provenance et à destination des États-Unis et l'approvisionnement en matières à double usage.

Dans une moindre mesure, le Canada se heurte aussi à des problèmes intérieurs qui peuvent mener à des actes extrémistes ou à des menaces de violence grave. La Ministre enjoint donc au SCRS de faire enquête et de conseiller le gouvernement du Canada au sujet des menaces que présentent :

- l'extrémisme religieux;
- le terrorisme d'État;
- la violence sécessionniste;
- l'extrémisme intérieur;
- le financement du terrorisme.

La Ministre enjoint aussi au Service de poursuivre ses recherches et analyses pour soutenir le processus d'inscription des entités terroristes; d'appuyer les déploiements du ministère de la Défense nationale; d'accroître sa capacité de liaison avec les partenaires étrangers; et de s'employer à poursuivre les membres d'organisations terroristes, à les expulser du Canada et à les empêcher de trouver refuge au pays, en collaboration avec d'autres ministères et organismes fédéraux.

La Ministre demande au SCRS de continuer à dépister les pays et groupes qui cherchent à élaborer des programmes de prolifération d'armes de destruction massive et autres

et, par la prestation de renseignements pertinents, à appuyer les obligations du Canada à endiguer l'acquisition de telles armes et les autres formes de prolifération. La Ministre note en outre les activités des pays qui recueillent de l'information sur le Canada et en sol canadien pour combler leurs besoins militaires, politiques et économiques. Le SCRS est tenu d'enquêter sur ces menaces, dont les activités influencées par l'étranger; la criminalité transnationale; les tentatives clandestines ou contraignantes de gouvernements étrangers de se procurer des renseignements, des informations ou des technologies exclusives; et celles visant à avoir accès à des informations ou à des infrastructures essentielles ou encore à les voler, à les abîmer ou à les détruire.

Selon les Exigences nationales, les évaluations de sécurité du Service, ses enquêtes de filtrage et ses conseils en matière de sécurité concernant les questions d'immigration et de citoyenneté sont des éléments importants de son mandat. Le SCRS est tenu de continuer à conseiller le gouvernement du Canada à ce sujet et de fournir des évaluations de sécurité concernant les processus de citoyenneté et d'immigration, les aéroports, la frontière terrestre, la sécurité maritime, la Cité parlementaire, les centrales nucléaires, les zones réglementées lors d'activités spéciales, les nominations par décret et certains gouvernements provinciaux.

Enfin, le SCRS est tenu de continuer à fournir au gouvernement du Canada des évaluations du renseignement à la fois pertinentes, complètes et non stratégiques et à suivre l'évolution rapide des nouvelles technologies. En plus de devoir améliorer le matériel technique et les systèmes d'information, le Service est invité à collaborer avec la GRC, le ministère de la Justice, Industrie Canada, le ministère de la Sécurité publique et de la Protection civile et d'autres ministères et organismes, à élaborer des mesures stratégiques et législatives visant à assurer que les lois canadiennes évoluent au même rythme que les technologies.

INSTRUCTIONS DU MINISTRE

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le Ministre peut donner des instructions au sujet des activités et des enquêtes du Service. L'instruction ministérielle énonçant les Exigences nationales en matière de renseignement de sécurité pour 2004-2005 est décrite ci-dessus. Aucune autre instruction n'a été donnée au cours de l'exercice à l'étude.

RÈGLEMENTS ET NOMINATIONS PAR LE GOUVERNEUR EN CONSEIL

En vertu du paragraphe 8(4) de la *Loi sur le SCRS*, le gouverneur en conseil peut établir pour le Service des règlements visant les pouvoirs et fonctions de son directeur ainsi que la conduite et la discipline de ses employés. Le gouverneur en conseil n'a instauré aucun règlement semblable au cours de 2004-2005.

MODIFICATIONS À LA POLITIQUE OPÉRATIONNELLE DU SCRS

La politique opérationnelle du SCRS fixe les paramètres et les règles qui s'appliquent à l'ensemble des activités d'ordre opérationnel du Service. Elle est mise à jour régulièrement suivant les changements législatifs et les instructions du Ministre. Le Comité étudie tous les changements qui y sont apportés pour assurer qu'ils respectent la loi et les instructions ministérielles. Il étudie aussi les politiques opérationnelles pertinentes et il évalue la conformité du SCRS à ces politiques lors de chacune de ses études.

Le Service a fait rapport au CSARS des politiques opérationnelles qui ont été inaugurées en 2004-2005 et de celles qui sont en cours d'élaboration ou de révision. Il a noté que les grands facteurs influençant ces progrès sont les modifications aux lois existantes, l'adoption de nouvelles lois et les changements à la méthode opérationnelle. Les politiques révisées en 2004-2005 touchent des sujets tels l'obtention de mandats en vertu de l'article 12 et les mises en garde faites lors de la communication d'informations et de renseignements opérationnels.

Le Service a fait rapport au CSARS des politiques opérationnelles qui ont été inaugurées en 2004-2005 et de celles qui sont en cours d'élaboration ou de révision.

Deux politiques étaient en cours d'élaboration en 2004-2005. La première concernait l'acquisition d'ordres de planification et la seconde, certains rapports opérationnels. Le Service a aussi signalé que diverses politiques existantes étaient en voie de révision durant la période à l'étude. Elles touchent des sujets tels le ciblage, la liaison et la coopération avec l'étranger, les pouvoirs conférés par la voie de mandats et l'approbation de ceux-ci, la coopération avec Citoyenneté et Immigration Canada et avec l'Agence des services frontaliers du Canada, et les rapports opérationnels.

De surcroît, le CSARS a obtenu du Service qu'il fasse le bilan des politiques en voie d'élaboration à la fin de l'exercice 2003-2004. Plusieurs d'entre elles ont été mises en œuvre depuis. Le SCRS a fait état d'une politique qui était toujours en cours d'élaboration parce qu'elle exigeait des consultations considérables et qu'elle était touchée par la restructuration de certains ministères. Un deuxième projet de politique, qui vise à revoir certaines procédures de communication de renseignements, était en plan à la fin de l'exercice.

C. Activités du SCRS sur le plan opérationnel

LUTTE CONTRE LA PROLIFÉRATION

La Direction de la lutte contre la prolifération (DLP) recueille des informations ayant trait aux programmes de mise au point d'armes biologiques, chimiques et nucléaires de gouvernements étrangers. Elle enquête en outre sur le terrorisme d'État.

La DLP est relativement nouvelle, ayant été créée en 2002. Aussi, en 2002-2003, le CSARS s'est-il engagé à mener des études approfondies sur ce groupe au cours des exercices suivants. En 2003-2004, il a étudié l'enquête du Service sur la menace que le programme d'armes de destruction massive d'un pays présentait pour la sécurité du Canada (*voir l'étude nº 2003-04 du CSARS*). En 2004-2005, le Comité a examiné une enquête de la DLP sur les actions d'un autre pays en matière d'armes de destruction massive.

La Sous-section des évaluations de la menace de la Direction prépare des rapports d'évaluation sur une vaste gamme de sujets. En 2004-2005, la DLP en a préparé 406, soit sensiblement moins que les 650 élaborés durant l'exercice précédent. Le SCRS a signalé que cette baisse était attribuable à divers facteurs, dont la révision des pratiques en matière de rapports, les changements de personnel et la création du Centre intégré d'évaluation des menaces (CIEM), qui a remplacé en 2004 le Centre intégré d'évaluation de la sécurité nationale de la Direction.

En 2004-2005, la DLP a préparé 406 rapports d'évaluation, soit sensiblement moins que les 650 élaborés durant l'exercice précédent.

Le Service a aussi donné au CSARS une séance d'information sur la création d'une nouvelle sous-section qui gère les enquêtes du Service sur certains programmes d'armes de destruction massive parrainés par des États étrangers et sur des activités liées à la prolifération.

Comme on peut le lire dans de précédents rapports annuels du CSARS, l'une des priorités de la DLP en 2004-2005 était l'enquête sur les efforts d'un certain pays pour améliorer ses programmes et capacités en matière d'armes de destruction massive.

La Direction a aussi élargi sa quête de renseignements sur les États commanditaires du terrorisme et sur les groupes terroristes qu'ils soutiennent. Elle a signalé au CSARS qu'elle avait réussi à identifier et à recruter des sources humaines et à les amener à lui faire rapport sur ces questions.

La Direction a fourni au CSARS de l'information sur le rôle joué par le SCRS à l'égard de la visite du président américain George W. Bush au Canada, en novembre 2004. Elle a travaillé en étroite collaboration avec les autres directions du Service et avec les partenaires gouvernementaux qui étaient chargés de la sécurité à cette occasion. La Sous-section des évaluations de la menace a préparé de nombreux rapports d'évaluation de menaces et la DLP a détaché du personnel au Centre national des opérations de la GRC pour la durée de la visite.

Le Service a aussi fait rapport des renseignements fournis à un organisme gouvernemental au sujet des efforts d'un certain pays pour se procurer des technologies d'exportation contrôlée. Des informations provenant à la fois de sources canadiennes et d'un service de renseignement étranger ont aussi appris au SCRS l'activité au Canada d'une institution qui pouvait avoir des liens avec une organisation terroriste.

ANTITERRORISME

La Direction de l'antiterrorisme (AT) a pour rôle de conseiller le gouvernement du Canada au sujet des nouvelles menaces de violence grave qui pourraient compromettre la sécurité des Canadiens et de leurs alliés. Ces menaces peuvent émaner du Canada ou de l'étranger.

Comme on a pu le lire dans les trois précédents rapports annuels du CSARS, le terrorisme islamique sunnite est demeuré le pôle principal des activités d'ordre opérationnel de la Direction de l'antiterrorisme. Une certaine restructuration a été effectuée pour faire face à la fluidité de cette priorité. Il y a aussi eu d'autres réaffectations à la Direction, au niveau de la supervision, en 2004-2005.

> Une nouvelle menace extrémiste qui s'intensifie au Canada et dans d'autres démocraties occidentales et dont les cibles sont dans la vingtaine, avisées sur le plan de la technologie et complètement occidentalisées.

On a en outre fait rapport d'une nouvelle menace extrémiste qui s'intensifie au Canada et dans d'autres démocraties occidentales et dont les cibles sont dans la vingtaine, avisées sur le plan de la technologie et complètement occidentalisées.

La Direction de l'AT a aussi fait rapport du soutien à la GRC et à un service de renseignement étranger. Elle a remis un total de 137 notes de communication en vertu de l'article 19 de la *Loi sur le SCRS* en 2004-2005. Cet article autorise le Service à communiquer, au personnel des services policiers, diplomatiques et voué à la défense du Canada, des informations recueillies dans l'exercice de ses fonctions. La Direction

a aussi fourni en détail au CSARS le nombre total de cibles individuelles et organisationnelles des enquêtes qui étaient en cours pendant l'exercice à l'étude.

En 2004-2005, le Comité a examiné les enquêtes antiterroristes et les conseils du SCRS au gouvernement au sujet du financement du terrorisme. Les résultats de ces études sont exposés dans le présent rapport. Le CSARS continuera d'étudier les enquêtes antiterroristes du SCRS en 2005-2006.

CONTRE-ESPIONNAGE

La Direction du contre-espionnage (CE) enquête sur les menaces que les activités de renseignement hostiles de gouvernements étrangers font peser sur la sécurité nationale. Ces activités peuvent comprendre l'espionnage, les activités influencées par l'étranger, la criminalité transnationale et les menaces à l'infrastructure sociale, politique et économique du Canada.

Le Service signale qu'il n'y a eu aucun changement structurel à la Direction et le Plan annuel de 2005-2006 n'a pas entraîné de modification aux priorités énoncées dans le plan annuel de l'exercice précédent. Le SCRS note que les activités d'espionnage des cibles du CE se font sans cesse plus complexes et astucieuses. Il a exposé au CSARS les mesures prises pour faire face à ces difficultés. La Direction du CE continue d'attacher une grande importance au recrutement de sources humaines pour maximiser son efficacité opérationnelle.

Au cours de l'exercice à l'étude, la Direction du CE n'a remis ni note de communication ni lettre d'autorisation en vertu de l'article 19.

Au cours de l'exercice à l'étude, la Direction du CE n'a remis ni note de communication ni lettre d'autorisation en vertu de l'article 19. Elle a informé le CSARS du nombre de cibles et du niveau des enquêtes autorisées; il s'agissait de cibles individuelles et organisationnelles et de cibles d'enquêtes contextuelles.

DIRECTION DE LA RECHERCHE, DE L'ANALYSE ET DE LA PRODUCTION

La Direction de la recherche, de l'analyse et de la production (RAP) est chargée d'élaborer des évaluations du renseignement de sécurité pour appuyer les opérations du Service et la prise de décisions par le gouvernement du Canada relativement aux menaces à la sécurité nationale. Vu la nature du contexte actuel de la sécurité et l'instantanéité de l'information, elle doit veiller à ce que l'information fournie aux décideurs soit exacte et leur parvienne en temps utile.

Au cours de l'exercice 2004-2005, la RAP a choisi de mettre l'accent sur la production d'analyses stratégiques et opérationnelles des menaces existantes et des problèmes nouveaux. *Bulletins de renseignements*, *Rapports* et *Études* demeurent les principaux documents qu'elle produit et diffuse largement au sein de la collectivité du renseignement de sécurité, dont le CSARS fait partie.

La participation d'autant de ressources de la RAP a permis de bien satisfaire aux exigences législatives du processus d'inscription, mais cela a entravé sa capacité à s'acquitter de ses responsabilités « normales » de recherche et de production.

En 2004-2005, la responsabilité de deux programmes a été réattribuée à la RAP. Cette direction est maintenant le pivot de la gestion de l'ensemble de l'information que le Service reçoit de l'un de ses grands alliés et de la diffusion ultérieure de cette information au nom des Directions de l'AT et du CE et de la DLP.

La RAP a assumé la responsabilité du processus d'inscription des entités terroristes cette année, au moment de l'examen biennal de ce processus. Comme on peut le lire dans l'étude nº 2004-03 du CSARS, elle a qualifié de « projet d'envergure » sa participation au premier examen biennal de la liste d'entités terroristes. Celui-ci a nécessité la participation de cinq bibliothécaires de recherche du Centre des opérations d'information, de douze analystes de la RAP et de quatre avocats. Cette direction estime qu'il a fallu environ dix jours pour effectuer les recherches et rédiger un RRS couvrant deux ans pour chacune des 35 entités inscrites. Elle a noté que la participation d'autant de ses ressources a permis de bien satisfaire aux exigences législatives du processus d'inscription, mais cela a entravé sa capacité à s'acquitter de ses responsabilités « normales » de recherche et de production.

Enfin, la RAP doit faire rapport des communications en vertu de l'article 19. Elle communique de l'information à la GRC en vertu de l'alinéa 19(2)*a*), ce qu'elle a fait à 155 reprises en 2004-2005. Les Directions de l'AT et du CE et la DLP ont fait rapport au CSARS de leurs communications aux organismes d'application de la loi en vertu de cet alinéa. Quant aux communications à Affaires étrangères Canada en vertu de l'alinéa 19(2)*b*), le Service a signalé qu'il y en avait eu 673 en 2004-2005. Enfin, on a relevé 384 communications au ministère de la Défense nationale en vertu de l'alinéa 19(2)*c*).

FILTRAGE DE SÉCURITÉ

Le paragraphe 13(1) de la *Loi sur le SCRS* autorise le Service à fournir des évaluations de sécurité aux institutions fédérales. À l'article 2 de la *Loi*, évaluation de sécurité est

Publications de la RAP

Les publications de la Direction de la recherche, de l'analyse et de la production (RAP) émanent d'un certain nombre de sources et sont rédigées sur la recommandation d'un analyste, par ordre d'un superviseur ou d'un gestionnaire de la RAP ou d'un cadre supérieur du SCRS, ou à la demande d'une direction opérationnelle, d'un bureau régional ou d'un client de l'extérieur. Voici comment se définissent ces publications.

Étude du SCRS

Étude analytique fondée sur une recherche approfondie de tous les éléments d'une menace donnée pour la sûreté au Canada. Il s'agit d'un document de référence à l'intention des directions à vocation opérationnelle du Service et de clients de l'extérieur. Les études du SCRS, qui comportent un sommaire, ne sont pas limitées quant à la longueur et sont généralement classifiées.

Rapport du SCRS

Document analytique qui est le fruit de recherches sur une menace donnée pour la sécurité et dont le Service a le mandat de s'occuper. Les rapports du SCRS fournissent des détails expliquant la nature de la menace aux lecteurs du SCRS et de l'extérieur. Ils sont normalement classifiés et peuvent compter jusqu'à huit pages.

Bulletin de renseignements

Document analytique concis qui a pour but de fournir aux clients de l'intérieur et de l'extérieur du Service une analyse d'une menace actuelle ou d'une question nouvelle entourant le mandat du SCRS. Les bulletins de renseignements sont normalement classifiés et peuvent compter jusqu'à trois pages.

Profil

Ce document, qui est destiné à fournir des informations pertinentes sur des pays, individus ou groupes auxquels le SCRS s'intéresse, est essentiellement un outil de travail pour les enquêteurs et les analystes opérationnels du Service. Normalement, il porte la cote de sécurité « Réservé à l'usage interne du SCRS » et ne peut être diffusé à l'extérieur sans que les informations délicates en aient été éliminées et que l'on ait consulté les directions opérationnelles. Les profils ne comptent pas plus de trois pages. Certains ne sont pas classifiés mais portent la mise en garde « Pour usage officiel seulement ».

Publications de la RAP *(suite)*

Fiche de renseignements

Les fiches de renseignements ont pour but de fournir des informations sur la structure organisationnelle passée ou actuelle de services étrangers de sécurité et de renseignement. Elles précisent les priorités de ces services en matière de collecte relativement au Canada ou en sol canadien. Les fiches servent aussi à informer sur des sujets précis, dont le crime organisé, les oligarques et les pays qui suscitent des préoccupations en matière de prolifération. Elles sont strictement réservées aux employés du SCRS.

Commentaire

Commentaire, dont la rédaction est confiée à des contractuels, fournit des informations sur un vaste éventail de sujets qui peuvent influer sur la sécurité du Canada. Il s'agit d'un document stratégique qui est largement diffusé au pays et à l'étranger et qui n'est pas classifié.

Rapport spécial

Ce document classifié, qui est destiné à un lectorat très restreint ou très précis, est habituellement rédigé en réponse à une demande d'intervention d'un ministère ou à la suite d'un événement.

ainsi défini : « évaluation de la loyauté d'un individu envers le Canada et, à cet égard, de sa fiabilité ». Quant aux paragraphes 13(2) et (3), ils habilitent le SCRS à conclure des ententes pour la prestation d'évaluations aux institutions et services de police provinciaux ainsi qu'aux gouvernements étrangers et aux institutions internationales.

En vertu des articles 14 et 15 de la *Loi sur le SCRS*, le Service effectue des enquêtes de sécurité et donne des avis à Citoyenneté et Immigration Canada (CIC) et à l'Agence des services frontaliers du Canada afin de les aider à traiter les demandes d'asile, d'immigration et de citoyenneté. Dans ces cas-là, ces avis sont fondés sur les catégories de personnes jugées interdites de territoire selon les critères de la *Loi sur l'immigration et la protection des réfugiés (LIPR)* en matière de sécurité. Le SCRS fournit aussi des évaluations de sécurité à CIC pour l'assister dans le filtrage des demandes de citoyenneté en vertu de l'article 19 de la *Loi sur la citoyenneté*.

En 2004-2005, le SCRS a reçu du gouvernement un total de 101 097 demandes d'habilitation de sécurité et d'autorisation d'« accès à des sites ». Il s'agit d'une hausse considérable par rapport aux 74 835 demandes traitées en 2003-2004. Il est aussi à noter qu'en 2004-2005 le Service a remis au gouvernement 39 notes d'information et

3 recommandations de refus d'habilitation de sécurité. Pendant la même période, il a reçu un total de 254 364 demandes de filtrage à l'immigration et à la citoyenneté et de contrôle préliminaire des réfugiés.

Au cours du dernier exercice, la Direction a subi un changement structurel pour ce qui est du traitement des demandes d'accès à des sites. Elle a signalé qu'il n'y avait eu aucune modification des priorités énoncées dans son plan annuel de 2004-2005 pour le filtrage de sécurité.

En 2004-2005, le SCRS a reçu du gouvernement un total de 101 097 demandes d'habilitation de sécurité et d'autorisation d'« accès à des sites ». Il s'agit d'une hausse considérable par rapport aux 74 835 demandes traitées en 2003-2004.

Tableau 2
Délais de filtrage des demandeurs d'asile et des candidats immigrants (2004-2005)

	Délai médian[16] (en jours civils)		
Programmes de filtrage de sécurité du SCRS	**Absence de renseignements défavorables**	**Notes d'information**	**Avis de non-admissibilité**
Contrôle préliminaire des réfugiés	27	336	248
Demandes de résidence permanente faites au Canada : programme de détermination du statut de réfugié	56	515	527
Demandes de résidence permanente faites au Canada : programme d'immigration	44	511	333
Demandes de résidence permanente faites aux États-Unis	150	599	642
Demandes de résidence permanente provenant de l'étranger (sauf les États-Unis)	7	531	236

16. Dans cette section du rapport annuel, le CSARS fait état des délais de traitement *médians*, et non moyens, des demandes d'évaluation par le Service. À son avis, cela représente de façon plus exacte le délai de traitement habituel en atténuant l'impact des délais de traitement anormalement brefs ou longs.

Habilitations de sécurité

Le Service a signalé avoir reçu 36 519 demandes d'habilitations de sécurité nouvelles ou de mise à jour d'habilitations existantes, soit une légère baisse par rapport aux 37 508 demandes de l'exercice précédent. En 2004-2005, il y a eu allongement notable des délais d'exécution des évaluations de niveaux I (Confidentiel) et II (Secret) pour le ministère de la Défense nationale (MDN), et une amélioration du délai d'exécution pour le MDN à l'égard des évaluations de niveau III (Très secret). Quant aux autres ministères et organismes fédéraux, il y a eu un léger allongement des délais d'exécution médians des évaluations de niveaux I et II et une amélioration de celui des évaluations de niveau III.

Le Service a signalé avoir reçu 36 519 demandes d'habilitations de sécurité nouvelles ou de mise à jour d'habilitations existantes, soit une légère baisse par rapport aux 37 508 demandes de l'exercice précédent.

Les temps médians du Service à fournir ses évaluations aux clients ministériels figurent au tableau 3.

Tableau 3
Délais d'exécution des évaluations de sécurité pour le secteur public

Catégorie	Niveau	Nombre médian de jours civils	
		2003-2004	2004-2005
MDN	I (Confidentiel)	20	49
	II (Secret)	18	63
	III (Très secret)	96	70
Autres ministères et organismes	I (Confidentiel)	7	12
	II (Secret)	11	14
	III (Très secret)	82	69

Programmes d'accès à des sites

Le Service a reçu un total de 64 578 demandes d'accès à des sites en 2004-2005. Il s'agit d'une hausse par rapport aux 28 822 demandes reçues en 2003-2004. De ce nombre, il en reçu 31 086 en vertu du *Programme d'autorisation d'accès aux zones réglementées d'aéroports*. Le temps de traitement médian de ces demandes par le Service a été de 24 jours civils.

Les 64 578 demandes traitées comprennent les 7 857 émanant de centrales nucléaires et de la Cité parlementaire (soit l'ensemble des installations relevant du Parlement du Canada). Le temps de traitement médian de ces demandes d'accès à des sites a été d'un jour civil. Les autres demandes (reçues d'autres ministères) ont été traitées en un jour civil.

Le Service a reçu un total de 64 578 demandes d'accès à des sites en 2004-2005. Il s'agit d'une hausse par rapport aux 28 822 demandes reçues en 2003-2004.

Tableau 4
Programmes d'accès à des sites

Programme	Nombre de demandes d'accès à des sites traitées	Temps de traitement médian (en jours civils)
Programme de la Cité parlementaire	1 110	1
Programme d'accès aux zones réglementées d'aéroports	31 086	24
Centrales nucléaires	6 747	1
Autres ministères	25 635	1

Filtrage au nom d'organismes étrangers

Le Service peut conclure des ententes réciproques avec des organismes étrangers afin de fournir des évaluations de sécurité au sujet de Canadiens et d'autres personnes qui ont résidé au Canada. En vertu de ces ententes, il ne leur recommande pas de refuser des habilitations de sécurité, mais il se borne à communiquer ses constatations au sujet des intéressés.

En 2004-2005, le Service a répondu à 869 demandes de filtrage au nom d'organismes étrangers, soit une diminution par rapport aux 1 208 vérifications effectuées en 2003-2004. Des enquêtes sur place ont été menées à l'égard de 151 de ces demandes.

Filtrage des demandeurs d'asile et des candidats immigrants

En 2004-2005, le SCRS a reçu 97 761 demandes de filtrage de demandeurs d'asile et de candidats à l'immigration, soit 3 529 de moins que durant l'exercice précédent. Il a remis aux fonctionnaires de l'Immigration un total de 232 notes d'information et de

En 2004-2005, le SCRS a reçu 97 761 demandes de filtrage de demandeurs d'asile et de candidats à l'immigration, soit 3 529 de moins que durant l'exercice précédent.

150 avis de non-admissibilité. Au cours de l'exercice précédent, le SCRS en avait remis 221 et 99, respectivement.

En 2004-2005, le Service a aussi donné 16 lettres d'anecdote et mis à jour 55 notes remises antérieurement à CIC. La description des types d'avis du SCRS à l'intention de CIC figure dans l'encadré de la page 70.

Le filtrage de sécurité des demandeurs d'asile et des candidats immigrants est effectué dans le cadre des trois programmes principaux qui figurent au tableau 5.

Tableau 5
Filtrage des demandeurs d'asile et des candidats immigrants (2004-2005)

Programmes de filtrage de sécurité du SCRS	Demandes reçues	Notes d'information	Avis de non-admissibilité
Contrôle préliminaire des réfugiés	22 871	115	69
Demandes de résidence permanente au Canada	38 628	84	65
Demandes de résidence permanente provenant de l'étranger (dont les renvois aux ALS)	36 262	33	16
Total	**97 761**	**232**	**150**

Contrôle de sécurité préliminaire des demandeurs d'asile

Le Programme de contrôle de sécurité préliminaire (PCSP), instauré en novembre 2001 par le gouvernement du Canada, aide à déceler, le plus tôt possible dans le processus de détermination du statut de réfugié, les risques que les demandeurs d'asile au Canada pourraient poser sur le plan de la sécurité. Pour 2004-2005, le Service a signalé avoir reçu 22 871 demandes en vertu de ce programme. Pendant la même période, il a donné des avis sur 22 227 dossiers, dont 115 notes d'information et 69 avis de non-admissibilité.

Pour 2004-2005, le Service a signalé avoir reçu 22 871 demandes en vertu du Programme de contrôle de sécurité préliminaire.

En vertu du PCSP, le délai médian du Service à fournir des avis d'absence de renseignements défavorables a été de 27 jours. Il a été de 336 et 248 jours pour les notes d'information et les avis de non-admissibilité, respectivement. Cela représente une légère augmentation sur les chiffres de l'exercice précédent qui étaient de 332 jours pour les notes d'information et de 214 pour les avis de non-admissibilité.

Demandes de résidence permanente présentées au Canada

Le Service a charge d'effectuer le filtrage sécuritaire de toutes les personnes qui demandent au Canada le statut de résident permanent. En 2004-2005, il a reçu 38 628 demandes de filtrage, dont 24 389 en vertu du programme d'immigration canadien et 14 239, du programme de détermination du statut de réfugié.

Les délais médians du Service à fournir ses avis dans ces dossiers a varié considérablement en 2004, selon que les demandes lui parvenaient sur papier ou par le système Échange de données informatisées (EDI). Le SCRS a noté que les échanges électroniques sont déjà bien établis pour le programme d'immigration canadien, à l'exception du filtrage des demandes d'immigration et de visa qui lui parviennent de l'étranger. Parmi les demandes de résidence permanente présentées au Canada, 95 p. 100 l'ont été par voie électronique (EDI). Pour 2004-2005, le délai de traitement médian a été de 33 jours pour les demandes reçues sur papier et de 45 pour les demandes par EDI.

Demandes de résidence permanente provenant de l'étranger

Pour les demandes de résidence permanente provenant de l'extérieur du Canada et des États-Unis, le Service partage la responsabilité du filtrage de sécurité avec les fonctionnaires de l'Immigration en poste dans les missions canadiennes à l'étranger. Dans ces dossiers, il ne prend part au processus que si le gestionnaire du Programme d'immigration lui en fait la demande. De cette façon, le SCRS peut se concentrer sur les dossiers présentant le plus de risques.

Au cours de la période à l'étude, le Service a reçu 5 408 demandes d'avis concernant le filtrage de demandes présentées aux bureaux de l'Immigration canadienne aux États-Unis.

Au cours de la période à l'étude, le Service a reçu 5 408 demandes d'avis concernant le filtrage de demandes présentées aux bureaux de l'Immigration canadienne aux États-Unis. Le délai de traitement médian de ces demandes a été de 25 jours civils pour celles présentées par EDI et de 288 jours pour les demandes sur papier.

Quarante-quatre pour cent des demandes d'immigration présentées aux États-Unis l'ont été par voie électronique. Le délai de traitement médian des dossiers de filtrage

de sécurité à l'immigration qui ont donné lieu à un *avis de vérification des données ou rien à signaler* a été de 150 jours.

Pour les demandes provenant de pays étrangers, sauf les États-Unis, le Service en a traité 26 430, dont 83 p. 100 par EDI. Le délai d'exécution médian a été de 38 jours civils pour les demandes sur papier et de 6 jours civils pour les demandes informatisées. De plus, les agents de liaison-sécurité du SCRS ont été consultés au sujet de 4 593 d'entre elles. Le Service a donné 17 notes d'information et 11 avis de non-admissibilité. Les délais de traitement médians ont été de 531 jours pour les notes d'information, de 236 pour les avis de non-admissibilité et de 7 jours pour les avis d'absence de renseignements défavorables.

Avis du SCRS à Citoyenneté et Immigration Canada (CIC)

Les évaluations du Service destinées au filtrage de sécurité sont fournies à CIC sous l'une des quatre formes suivantes :

- *Avis de vérification des données/rien à signaler :* rapport remis à CIC si le Service n'a aucun renseignement défavorable sur le demandeur.

- *Avis de non-admissibilité :* fourni dans les cas où le SCRS conclut, d'après les renseignements dont il dispose, que le demandeur répond aux critères d'interdiction de territoire énoncés dans les dispositions de la *LIPR* concernant la sécurité.

- *Note d'information :* affirme que le Service détient des informations selon lesquelles le demandeur trempe ou a trempé dans des activités visées par les dispositions de la *LIPR* ayant trait à la sécurité, mais précise que l'intéressé n'entre pas dans la catégorie des personnes interdites de territoire en vertu de cette loi.

- *Lettre d'anecdote :* remise à CIC par le SCRS si celui-ci détient des informations voulant que le demandeur prenne ou ait pris part à des activités étrangères à la sécurité et décrites dans la *LIPR* (crimes de guerre ou criminalité organisée, par exemple) ou s'il veut signaler toute autre question ayant trait à l'exercice des fonctions du ministre de la Citoyenneté et de l'Immigration, conformément à l'alinéa 14*b*) de la *Loi sur le SCRS*.

Direction de la liaison avec l'étranger et des visites

La Direction de la liaison avec l'étranger et des visites (LEV) est chargée d'assurer la liaison du Service avec les organismes étrangers. Elle recourt aux voies de liaison pour échanger de l'information sur les menaces envers la sécurité du Canada.

En vertu du paragraphe 17(1) de la *Loi sur le SCRS*, le Service peut, pour exercer ses fonctions, conclure des ententes avec des États étrangers, y compris avec des gouvernements étrangers ou des organisations internationales d'États ou leurs institutions. Les instructions ministérielles et la politique opérationnelle du SCRS énoncent les principes régissant la conclusion et la gestion de ces ententes, mais c'est la portée d'une entente avec un organisme étranger qui détermine la nature et l'ampleur de la coopération et des échanges du Service avec lui. La portée de l'entente détermine aussi le type particulier de partage d'information qui peut être fait.

À la fin de 2004-2005, le Service avait conclu 257 ententes avec des organismes de 143 pays.

À la fin de 2004-2005, le Service avait conclu 257 ententes avec des organismes de 143 pays. Durant cet exercice, il a été autorisé par le Ministre à en établir dix nouvelles et il a demandé une autorisation à l'égard de deux autres ententes. Le SCRS a aussi modifié ou élargi une entente avec un organisme étranger et demandé l'autorisation ministérielle en vue d'en élargir trois autres.

Des 257 ententes conclues par le Service avec des organismes étrangers, 42 étaient considérées comme inappliquées (terme qui s'entend de l'absence de liaison pendant au moins un an). Le SCRS maintient des restrictions à l'égard des échanges d'information dans le cas de cinq de ces ententes inappliquées, en raison :

- de craintes suscitées par le bilan de l'organisme étranger intéressé en matière de respect des droits de la personne;
- d'un ou de plusieurs manquements à l'interdiction de communiquer de l'information à des tiers; ou
- de la piètre fiabilité générale du contact pour la liaison.

Le Service peut choisir de réactiver des ententes inappliquées dans les cas où peuvent survenir des conflits régionaux et des événements politiques susceptibles d'affecter les impératifs du Canada en matière de sécurité nationale.

La Direction de la LEV a aussi charge des bureaux de liaison-sécurité. Dans le cadre de son Programme de liaison avec l'étranger, le Service a des bureaux de liaison-sécurité à l'extérieur du pays qui partagent généralement les locaux de missions diplomatiques canadiennes. Il mise beaucoup sur ces bureaux pour évaluer l'utilité de chacune des ententes conclues avec des organismes étrangers en vertu de l'article 17 et la fiabilité de ceux-ci. Ces bureaux procurent aussi une aide considérable à Citoyenneté et Immigration Canada quant aux besoins de filtrage à l'immigration liés aux articles 14 et 15 *(voir le Rapport nº 2004-01 dans le présent rapport annuel)*.

La Direction de la LEV coordonne aussi les visites de représentants d'organismes étrangers, dont les ambassadeurs étrangers, à l'Administration centrale et aux bureaux régionaux du SCRS, et les voyages des représentants de celui-ci à l'étranger.

ENTENTES DU SCRS AVEC DES ORGANISMES CANADIENS

L'exécution du mandat du Service en vertu des articles 12 à 16 de la *Loi sur le SCRS* requiert une coopération courante entre les gouvernements aux niveaux fédéral et provincial et avec les services de police d'une province donnée. La coopération peut prendre la forme d'échanges d'information, d'aide opérationnelle ou d'opérations conjointes. Le SCRS n'a pas besoin d'accord officiel pour communiquer de l'information à un ministère, à un organisme gouvernemental ou à un service de police canadiens en raison de la responsabilité qui lui incombe de conseiller le gouvernement. Les renseignements classifiés, transmis dans ces circonstances à un ministère ou à un organisme fédéral, sont protégés par les dispositions normales de la Politique du gouvernement sur la sécurité.

Le SCRS a conclu un accord avec le conseiller du premier ministre à la sécurité nationale, au Bureau du Conseil privé, pour la création et la gestion du Centre intégré d'évaluation des menaces.

Cependant, en vertu de l'alinéa 17(1)*a)* de la *Loi sur le SCRS*, le Service peut, avec l'approbation du Ministre, conclure par écrit avec des organismes canadiens, des accords de coopération appelés protocoles d'entente, afin d'exercer ses fonctions.

Au cours de l'exercice à l'étude, le SCRS a conclu un accord avec le conseiller du premier ministre à la sécurité nationale, au Bureau du Conseil privé, pour la création et la gestion du Centre intégré d'évaluation des menaces, ce qui donne un total de 17 accords semblables avec des institutions fédérales. Le nombre d'ententes conclues avec des organismes des provinces (10) est demeuré inchangé. Il n'y a eu aucune résiliation ni modification d'ententes existantes.

Relations avec la GRC

Au nombre des ententes avec des organismes canadiens, le protocole d'entente entre le SCRS et la GRC occupe une très large place dans l'étude du CSARS en raison du volume des échanges entre ces deux organismes et de leur partage suivi d'opérations conjointes.

En 2004-2005, il y a eu 855 échanges d'information écrits ou verbaux de la GRC avec le Service, soit une hausse considérable par rapport aux 615 de l'exercice précédent. Pour sa part, le SCRS a fourni à la GRC 227 notes de communication en 2004-2005, contre 215 au cours de l'exercice précédent. Pour autoriser la GRC à utiliser ses renseignements dans une enquête criminelle, le Service lui remet une note de communication.

Au cours de 2004-2005, le SCRS a aussi donné à la GRC 24 lettres d'autorisation, contre 15 en 2003-2004. La GRC lui demande de telles lettres pour être autorisée à utiliser ses renseignements dans des poursuites judiciaires.

En 2004-2005, il y a eu 855 échanges d'information écrits ou verbaux de la GRC avec le Service, soit une hausse considérable par rapport aux 615 de l'exercice précédent.

L'exercice à l'étude marque la quatrième année de fonctionnement des Équipes intégrées de la sécurité nationale (EISN), dirigées par la GRC, auxquelles sont détachés des employés de quatre régions et de l'Administration centrale du SCRS. Le Service signale que les EISN ont été utiles du fait qu'elles ont resserré la coopération entre le Service et la GRC. Comme elles sont dirigées par celle-ci sur le plan opérationnel, le CSARS a une capacité très limitée d'en examiner les activités et, en fait, ces opérations conjointes font encore une fois ressortir les limites de son mandat dans le secteur de la sécurité, qui est de plus en plus intégré sur le plan opérationnel.

Cette année, le CSARS a mené deux études (2004-02 et 2004-07) sur le fond de l'information échangée par le Service avec la GRC et sur la nature de leur coopération mutuelle, lors de ses examens des bureaux régionaux et des enquêtes du SCRS.

MANDATS DE LA COUR FÉDÉRALE : GÉNÉRALITÉS ET STATISTIQUES

Outre leur caractère fort intrusif, les mandats sont l'un des instruments les plus puissants qui soient mis à la portée du gouvernement du Canada. Ils procurent aux organismes intéressés l'autorisation de la Cour fédérale à employer des méthodes d'enquête qui seraient autrement illégales, par exemple l'interception de communications téléphoniques. Pour cette seule raison, l'utilisation de mandats par le Service justifie une surveillance constante, tâche que le Comité prend très au sérieux. Au fil de l'étude approfondie des enquêtes du SCRS par le CSARS, chaque mandat (et ses pièces justificatives) est généralement l'objet d'un examen détaillé.

Tableau 6
Mandats nouveaux et remplacés, renouvelés ou supplémentaires

	2002-2003	2003-2004	2004-2005
Mandats nouveaux	52	68	40
Mandats remplacés, renouvelés ou supplémentaires	150	130	207
Total	**202**	**198**	**247**[17]

Chaque année, le Comité invite le Service à lui fournir des statistiques sur ses demandes de mandat à la Cour fédérale (dans lesquelles il communique des informations au tribunal) et sur les mandats que celle-ci lui décerne. Le tableau 6 fournit une comparaison du nombre des mandats qui ont été décernés au cours de chacun des trois derniers exercices.

En 2004-2005, la plupart des mandats ont été approuvés pour un an. Un petit nombre d'entre eux l'ont été pour une période plus brève, à la demande du Service. L'idée était d'en faire coïncider la date d'expiration avec celle d'autres mandats liés à des dossiers connexes.

L'utilisation de mandats par le Service justifie une surveillance constante, tâche que le Comité prend très au sérieux.

Le CSARS a appris qu'en 2004-2005, la plupart des mandats avaient été approuvés pour un an. Un petit nombre d'entre eux l'avaient été pour une période plus brève, à la demande du Service. L'idée était d'en faire coïncider la date d'expiration avec celle d'autres mandats liés à des dossiers connexes.

Dans le cas de trois demandes, la Cour a demandé au Service des rapports provisoires destinés à lui fournir des renseignements à jour sur l'état d'une cible ou à justifier la nécessité ou l'utilité soutenue des mandats.

Dans un autre cas, la Cour a refusé d'octroyer un des pouvoirs demandés par le Service tant qu'on ne lui aurait pas fourni de preuve plus convaincante de la nécessité de ce pouvoir.

17. L'augmentation du total des mandats traduit une nouvelle façon de compiler les statistiques et non une hausse au titre du ciblage.

À plusieurs reprises, des révisions ont été faites aux affidavits appuyant des demandes de mandat lors d'audiences de la Cour fédérale. En une occasion, la Cour a ajourné l'audience pour permettre au Service d'apporter des changements. La demande a été approuvée sur présentation des documents modifiés.

La Cour fédérale n'a imposé aucune condition nouvelle ni modifié de conditions existantes pour les mandats au cours de l'exercice à l'étude. Le Service a aussi signalé qu'aucune décision judiciaire n'avait eu de portée sur ses demandes de mandats ou sur l'exécution des pouvoirs conférés par ceux-ci, ni sur le processus des mandats en général en 2004-2005.

Selon le Service, la Cour fédérale a octroyé 9 mandats urgents en 2004-2005, contre 30 pendant l'exercice précédent.

Il faut aussi noter que l'article 28 de la *Loi sur le SCRS* autorise le gouverneur en conseil à établir des règlements applicables aux aspects suivants : les formes des mandats; la pratique et la procédure applicables à l'audition des demandes; ainsi que les lieux où les audiences peuvent être tenues et la forme qu'elles peuvent prendre. Aucun règlement n'a été établi en 2004-2005.

Section 3

Vous souhaitez en savoir plus? Coup d'œil sur le CSARS

Vous souhaitez en savoir plus? Coup d'œil sur le CSARS

COMPOSITION DU COMITÉ

Au cours de l'exercice 2004-2005, la présidence du Comité était occupée par l'honorable Paule Gauthier, C.P., O.C., O.Q., c.r., qui a accédé pour la première fois à cette charge le 30 septembre 1996, puis s'est vu confier en 2000 un second mandat de cinq ans. Son dernier mandat à la présidence a pris fin le 7 juin 2005. Le 24 du même mois, l'honorable Gary Filmon, C.P., O.M., a été nommé à titre de nouveau président du CSARS et M^me^ Aldéa Landry, C.P., c.r., est devenue le tout dernier membre du Comité. Les autres membres sont l'honorable Raymond Speaker, C.P., O.C. (nommé pour un nouveau mandat de cinq ans le 16 septembre 2004), l'honorable Baljit Chadha, C.P. et l'honorable Roy Romanow, C.P., O.C., c.r.

Tous les membres du Comité font partie du Conseil privé et sont nommés par le gouverneur en conseil après consultation entre le premier ministre et les chefs des partis de l'opposition. Aucun poste n'était vacant au CSARS à la fin de l'exercice à l'étude.

PERSONNEL ET ORGANISATION

Le Comité jouit du soutien d'un directeur exécutif et d'un effectif de 19 employés, en poste à Ottawa. Son personnel est ainsi composé : un directeur exécutif associé, un sous-directeur exécutif, un avocat principal, un avocat, un parajuriste principal (aussi agent/analyste à l'accès à l'information et à la protection des renseignements personnels), neuf recherchistes, un directeur des services généraux et quatre employés de soutien administratif.

Le 24 juin 2005, l'honorable Gary Filmon, C.P., O.M., a été nommé à titre de nouveau président du CSARS et M^me^ Aldéa Landry, C.P., c.r., est devenue le tout dernier membre du Comité.

Les membres du Comité dictent au personnel l'orientation à donner aux travaux de recherche et aux autres activités qui sont désignés prioritaires pour l'année. La marche des activités courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir, auprès du président, premier dirigeant du CSARS.

ACTIVITÉS DE RECHERCHE ET DE SURVEILLANCE

Chaque année, le Comité choisit diverses enquêtes et un certain nombre de secteurs confiés au SCRS afin de les scruter en profondeur. Par suite d'événements imprévus ou de priorités nouvelles, des projets supplémentaires peuvent venir s'ajouter à ces études. Les analystes du CSARS effectuent des recherches approfondies pour chaque projet et, à cet égard, ils reçoivent des directives de la haute direction et rendent compte régulièrement aux membres du Comité. Étant donné la cote de sécurité élevée et le caractère délicat des documents examinés, le personnel répartit son temps entre les bureaux du CSARS et un local entièrement équipé qui est voué à son usage exclusif, à l'Administration centrale du SCRS.

EXPOSÉS SUR LE RENSEIGNEMENT DE SÉCURITÉ

Dans le cadre de leur quête suivie d'information, le président et les membres du Comité ainsi que les cadres supérieurs prennent part à des discussions régulières avec la direction et le personnel du SCRS et avec d'autres membres de haut rang de la collectivité du renseignement de sécurité. À ces échanges se greffent des discussions avec des universitaires, des experts du renseignement et de la sécurité et des organismes non gouvernementaux compétents, tels des groupes de défense des droits de la personne. Ces activités ont pour but de mieux faire connaître au CSARS l'éventail des dossiers et opinions qui intéressent le domaine du renseignement de sécurité. Les membres du Comité visitent aussi à tour de rôle les bureaux régionaux du Service pour examiner l'incidence que les instructions ministérielles et la politique du SCRS ont sur le travail courant des enquêteurs locaux. Ces voyages leur fournissent l'occasion de rencontrer les cadres supérieurs du Service, d'entendre des exposés sur les problèmes, difficultés, priorités et perspectives propres à ces bureaux et d'exposer ce qui polarise les efforts et les préoccupations du CSARS. Au cours de l'exercice 2004-2005, le Comité s'est rendu dans deux bureaux régionaux.

AUTRES ACTIVITÉS DU COMITÉ

- Le 8 septembre 2004, le directeur exécutif du CSARS a entretenu les membres du comité parlementaire provisoire qui avait été créé et chargé de consulter et de formuler des recommandations au sujet du comité parlementaire de la sécurité nationale, qui était proposé dans la loi.

- La présidente, les membres et le directeur exécutif du Comité ont assisté à la conférence internationale des organismes de surveillance du renseignement à Washington, D.C., du 3 au 5 octobre 2004. Ils y sont demeurés une journée de plus pour rencontrer les représentants d'organes de contrôle de la collectivité américaine du renseignement de sécurité.

- Le 6 octobre 2004, le haut-commissaire de Grande-Bretagne est venu aux bureaux du CSARS présenter le nouveau chef du British Security Intelligence Service, nommé en août 2004.

- Le directeur exécutif associé a été invité à prononcer une conférence au nom du directeur exécutif à un séminaire sur le renseignement, l'habileté politique et les affaires internationales que le Canadian Centre of Intelligence and Security Studies de l'Université Carleton a donné le 6 octobre 2004. Il a alors brossé un tableau d'ensemble du CSARS aux étudiants.

- Le directeur exécutif a assisté à la conférence que le Canadian Centre of Intelligence and Security Studies a tenue à Ottawa les 14 et 15 avril 2004 sur l'affaire Gouzenko, qui a amorcé l'histoire du contre-espionnage canadien et de la guerre froide dans le domaine du renseignement. Le directeur exécutif est membre du conseil consultatif du Canadian Centre.

- Le directeur exécutif et plusieurs cadres ont assisté à une conférence que l'Association canadienne pour l'étude de la sécurité et du renseignement a tenue à Ottawa du 14 au 17 octobre 2004.

- Le 26 novembre 2004, le directeur exécutif et le sous-directeur exécutif ont rencontré les membres du comité de surveillance des services de renseignement et de sécurité des Pays-Bas.

- Le 21 mars 2005, le directeur exécutif a donné un exposé aux étudiants inscrits au cours de l'Université Carleton sur la sécurité nationale et le renseignement dans l'État moderne.

- Au printemps 2005, le CSARS a publié le document *Réflexions*, qui rappelle les événements décisifs de ses 20 années d'histoire, dont la Commission McDonald et l'adoption de la *Loi sur le SCRS* ainsi que les principales études et les importants dossiers de plaintes qu'il a eu à traiter au cours des deux dernières décennies. Cette publication fournit en outre des renseignements détaillés sur le fonctionnement interne du Comité, ce qui contribue à sensibiliser le public sur son rôle et ses responsabilités.

BUDGET ET DÉPENSES

Le Comité continue de gérer ses activités dans les limites des ressources qui lui sont attribuées. Le traitement et les déplacements de son personnel au Canada, pour les audiences et les séances d'information ainsi que pour ses activités d'examen, constituent ses principales dépenses. En décembre 2004, le Parlement a approuvé un budget supplémentaire des dépenses qui a majoré de 344 000 $ le budget du CSARS pour l'exercice 2004-2005 et chacun des suivants. Cela donnait suite à une présentation faite au Conseil du Trésor en 2002 par le Comité et présentant une analyse de rentabilité qui montrait pourquoi il avait besoin de crédits supplémentaires pour suivre une hausse de 30 p. 100 du budget du SCRS. Ces nouveaux crédits ont surtout servi à embaucher de nouveaux recherchistes. Le tableau 7 présente une ventilation des dépenses réelles et prévues.

Tableau 7
Défenses du CSARS

	2004-2005 (dépenses réelles)	2005-2006 (prévisions)
Personnel	1 766 330	1 777 000
Fonctionnement	886 822	1 019 000
Total	**2 653 152**	**2 796 000**

DEMANDES EN VERTU DES *LOIS SUR L'ACCÈS À L'INFORMATION* ET *SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Le public peut présenter au CSARS des demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. Le tableau 8, « Demandes de communication de renseignements », fait état du nombre des demandes que ces lois ont values au Comité au cours des trois derniers exercices.

Les demandes d'accès à l'information concernant les études du Comité forment l'essentiel de l'ensemble de ces demandes. Le travail que requiert la préparation d'un rapport en vue de le rendre public n'a besoin d'être fait qu'une seule fois, mais il profite à toutes les personnes qui demandent le rapport. Voilà pourquoi le CSARS ne perçoit pas de droits à l'égard des demandes d'accès à ses études.

Tableau 8
Demandes de communication de renseignements

Exercice	*Loi sur l'accès à l'information*	*Loi sur la protection des renseignements*
2002-2003	20	4
2003-2004	31	1
2004-2005	21	3

LA FONCTION DE CONTRÔLEUR MODERNE

Le CSARS a fait de grands progrès dans la mise en œuvre des initiatives entourant la fonction de contrôleur moderne au cours de l'exercice à l'étude. Il a d'abord mené à terme un plan d'action en matière de gestion, une évaluation du risque et un plan de vérification, puis il a élaboré des indicateurs de rendement. D'autres travaux destinés à appuyer la mise en œuvre de cette fonction se poursuivront au cours du prochain exercice. En raison de son petit effectif et de l'impossibilité d'embaucher des experts fonctionnels, le CSARS doit souvent faire appel à des ressources de l'extérieur afin d'obtenir l'expertise requise pour cette initiative.

Annexe A

Sigles employés dans le rapport

Sigles employés dans le rapport

ALS	Agent de liaison-sécurité
AT	Antiterrorisme
CE	Contre-espionnage
CIC	Citoyenneté et Immigration Canada
CIEM	Centre intégré d'évaluation des menaces
CIESN	Centre intégré d'évaluation de la sécurité nationale
COI	Centre des opérations d'information
CSARS	Comité de surveillance des activités de renseignement de sécurité
CT	Criminalité transnationale
DLP	Direction de la lutte contre la prolifération
EDI	Échange de données informatisées
EISN	Équipes intégrées de la sécurité nationale
GRC	Gendarmerie royale du Canada
IET	Inscription des entités terroristes
IG	Inspecteur général
LEV	Liaison avec l'étranger et Visites
LIPR	*Loi sur l'immigration et la protection des réfugiés*
MDN	Ministère de la Défense nationale

PCSP	Programme de contrôle de sécurité préliminaire
RAP	Recherche, analyse et production
RARNULT	*Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme*
RRS	Rapport de renseignements de sécurité
SCRS	Service canadien du renseignement de sécurité
SPPC	Sécurité publique et Protection civile

Annexe B

Rapports et études du CSARS depuis 1984

Rapports et études du CSARS depuis 1984

(Les rapports présentés aux termes de l'article 54, soit les rapports spéciaux du Comité au Ministre, sont marqués d'un astérisque.)

1. *Dix-huit mois après la séparation : une appréciation de la conception du SCRS sur le recrutement, le perfectionnement et les questions connexes* (SECRET)* (86/87-01)

2. *Rapport d'une étude portant sur le filtrage de sécurité des fonctionnaires et des personnes postulant un emploi dans la fonction publique fédérale* (SECRET)* (86/87-02)

3. *Le réseau du renseignement et de sécurité au sein de l'administration gouvernementale du Canada : une description* (SECRET)* (86/87-03)

4. *Alerte de sécurité à l'aéroport d'Ottawa* (SECRET)* (86/87-05)

5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions* (SECRET)* (87/88-01)

6. *Pour corriger une situation : langues officielles et relations de travail au sein du SCRS* (NON CLASSIFIÉ)* (86/87-04)

7. Counter-Subversion: SIRC Staff Report (SECRET) (87/88-02)

8. *Rapport du CSARS — Sélection des immigrants* (SECRET)* (87/88-03)

9. *L'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier* (VERSION PUBLIQUE)* (87/88-04)

10. *La Direction de l'évaluation du renseignement : une revue par le CSARS du processus de production* (SECRET)* (88/89-01)

11. *CSARS — Examen du programme de l'antiterrorisme du SCRS* (TRÈS SECRET)* (88/89-02)

12. *Rapport présenté au Solliciteur général du Canada sur la protection des biens scientifiques et techniques au Canada : le rôle du SCRS* (SECRET)* (89/90-02)

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (SECRET)* (89/90-03)

14. *L'examen de la politique et des pratiques du SCRS concernant les divulgations non autorisées d'informations classifiées* (SECRET) (89/90-04)

15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information* (SECRET)* (89/90-05)

16. *Modifications à la* Loi sur le SCRS *: propositions au Comité spécial de la Chambre des communes* (NON CLASSIFIÉ) (89/90-06)

17. *Rapport sur l'entrevue concernant les Innus et l'enquête sur l'extrémisme autochtone* (SECRET)* (89/90-07)

18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988* (SECRET)* (89/90-01)

19. *A Review of the Counter-Intelligence Program in the CSIS* (TRÈS SECRET)* (89/90-08)

20. *Échanges de renseignements avec des organismes canadiens* (SECRET)* (90/91-03)

21. *Cibles établies en vertu de l'alinéa 2d) — une étude du CSARS sur les opérations restantes de la Direction de l'antisubversion* (SECRET) (90/91-06)

22. *Études régionales (six études sur une région)* (TRÈS SECRET) (90/91-04)

23. *Study of CSIS' Policy Branch* (CONFIDENTIEL) (90/91-09)

24. *Enquêtes, affectation de sources et rapport sur les cibles en vertu de l'alinéa 2b)* (TRÈS SECRET) (90/91-05)

25. *Communication de renseignements aux services étrangers* (TRÈS SECRET)* (90/91-02)

26. *Examen par le CSARS des activités du SCRS touchant les Canadiens autochtones* (SECRET)* (90/91-07)

27. *Enquêtes de sécurité sur les campus universitaires* (TRÈS SECRET)* (90/91-01)

28. *Report on Multiple Targeting* (SECRET) (90/91-08)

29. *Revue de l'enquête sur Bull, la Corporation de recherche spatiale et l'Iraq* (SECRET) (91/92-01)

30. *Rapport sur l'immigration d'Al Mashat au Canada* (SECRET)* (91/92-02)

31. *East Bloc Investigations* (TRÈS SECRET) (91/92-08)

32. *Review of CSIS Activities Regarding Sensitive Institutions* (TRÈS SECRET) (91/92-10)

33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)

34. *Échange d'informations et de renseignements entre le Service canadien du renseignement de sécurité et le Centre de la sécurité des télécommunications* (TRÈS SECRET)* (91/92-04)

35. *Victor Ostrovsky* (TRÈS SECRET) (91/92-05)

36. *Report on Two Iraqis — Ministerial Certificate Case* (SECRET) (91/92-06)

37. *Évaluations de la menace, étude en vertu de l'article 40* (SECRET)* (91/92-07)

38. *L'attaque contre l'ambassade de l'Iran à Ottawa* (TRÈS SECRET)* (92/93-01)

39. *"STUDYNT" The Second CSIS Internal Security Case* (TRÈS SECRET) (91/92-15)

40. *Les cibles du terrorisme national — un examen du CSARS* (TRÈS SECRET)* (90/91-13)

41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)

42. *The Audit of Section 16 Investigations* (TRÈS SECRET) (91/92-18)

43. *Activités du SCRS pendant la Guerre du Golfe : entrevues dans la communauté* (SECRET) (90/91-12)

44. *Examen de l'enquête menée par le SCRS sur un agent clandestin latino-américain — un examen du CSARS* (TRÈS SECRET)* (90/91-10)

45. *Les activités du SCRS relativement à la destruction de l'avion affecté au vol 182 d'Air India le 23 juin 1985 — un examen du CSARS* (TRÈS SECRET)* (91/92-14)

46. *Région des Prairies — rapport sur les autorisations d'enquête (chapitre 1)* (TRÈS SECRET)* (90/91-11)

47. *L'attentat contre Hassan El-Tourabi* (SECRET) (92/93-07)

48. *Domestic Exchanges of Information (A SIRC Review — 1991/92)* (SECRET) (91/92-16)

49. *Vérification de la région des Prairies* (TRÈS SECRET) (90/91-11)

50. *La présumée venue du sheikh Rahman à Ottawa* (SECRET) (AT 93-06)

51. *Regional Audit* (TRÈS SECRET)

52. *Examen par le CSARS des bureaux des ALS du Service (Londres et Paris)* (SECRET) (91/92-11)

53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)

54. *Intelligence-Source Confidentiality* (TRÈS SECRET) (CI 93-03)

55. *Domestic Investigations (1)* (SECRET) (CT 93-02)

56. *Enquêtes menées au Canada (2)* (TRÈS SECRET) (AT 93-04)

57. *Middle East Movements* (SECRET) (CT 93-01)

58. *A Review of CSIS' SLO Posts (1992-93)* (SECRET) (CT 93-05)

59. *Review of Traditional CI Threats* (TRÈS SECRET) (CI 93-01)

60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)

61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)

62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)

63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 93-11)

64. *Sources in Government* (TRÈS SECRET) (CI 93-09)

65. *Regional Audit* (TRÈS SECRET) (CI 93-02)

66. *The Proliferation Threat* (SECRET) (CT 93-07)

67. *L'Affaire du Heritage Front, rapport présenté au Solliciteur général du Canada* (SECRET)* (AT 94-02)

68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)

69. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1993-1994)* (SECRET) (CE 93-08)

70. *The Proliferation Threat — Case Examination* (SECRET) (CT 94-04)

71. *Community Interviews* (SECRET) (CT 93-11)

72. *Une enquête suivie en matière de contre-espionnage* (TRÈS SECRET)* (CE 93-07)

73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)

74. *A SIRC Review of CSIS' SLO Posts (1994-95)* (SECRET) (CT 95-01)

75. *Regional Audit* (TRÈS SECRET) (CI 93-10)

76. *Terrorism and a Foreign Government* (TRÈS SECRET) (CT 94-03)

77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)

78. *Review of Certain Foreign Intelligence Services* (TRÈS SECRET) (CE 94-02)

79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 94-01)

80. *Échanges d'information avec des organismes canadiens* (enquête du CSARS 1994-1995) (SECRET) (CE 94-03)

81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)

82. *CSIS and a "Walk-In"* (TRÈS SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TRÈS SECRET) (CI 95-02)

84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 95-05)

85. *Vérification régionale* (TRÈS SECRET) (AT 95-02)

86. *A Review of Investigations of Emerging Threats* (TRÈS SECRET) (CI 95-03)

87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)

88. *Homeland Conflict* (TRÈS SECRET) (CT 96-01)

89. *Vérification régionale* (TRÈS SECRET) (CE 96-01)

90. *La gestion des sources humaines* (TRÈS SECRET) (CE 96-03)

91. *Economic Espionage I* (SECRET) (CI 96-02)

92. *Economic Espionage II* (TRÈS SECRET) (CI 96-02)

93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-1997* (TRÈS SECRET) (CI 96-04)

94. *Urban Political Violence* (SECRET) (SIRC 1997-01)

95. *Domestic Exchanges of Information (1996-97)* (SECRET) (SIRC 1997-02)

96. *Conflit étranger*, partie I (SECRET) (CSARS 1997-03)

97. *Regional Audit* (TRÈS SECRET) (SIRC 1997-04)

98. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1997-05)

99. *Spy Case* (TRÈS SECRET) (SIRC 1998-02)

100. *Enquêtes menées au Canada* (TRÈS SECRET) (CSARS 1998-03)

101. Coopération du SCRS avec la Gendarmerie royale du Canada — partie I (SECRET)* (CSARS 1998-04)

102. *Source Review* (TRÈS SECRET) (SIRC 1998-05)

103. *Interagency Cooperation Case* (TRÈS SECRET) (SIRC 1998-06)

104. *A Case of Historical Interest* (TRÈS SECRET) (SIRC 1998-08)

105. *Le rôle du SCRS dans le filtrage de sécurité des demandes d'immigration* (SECRET) (AT 95-06)

106. *Un conflit étranger*, partie II (TRÈS SECRET) (CSARS 1997-03)

107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)

108. *Coopération du SCRS avec la GRC — partie II* (SECRET)* (CSARS 1998-04)

109. *Audit of Section 16 Investigations and Foreign Intelligence 1997-98* (TRÈS SECRET) (SIRC 1998-07)

110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)

111. *Regional Audit* (TRÈS SECRET) (SIRC 1998-10)

112. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1998-11)

113. *Allégations d'un ancien employé du SCRS* (TRÈS SECRET)* (CSARS 1998-12)

114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)

115. *Review of Foreign Intelligence Activities in Canada* (TRÈS SECRET) (SIRC 1998-15)

116. *Files* (TRÈS SECRET) (SIRC 1998-16)

117. *Audit of Section 16 Investigations and Foreign Intelligence* (TRÈS SECRET) (SIRC 1999-01)

118. *A Long-Running Counter Intelligence Investigation* (TRÈS SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TRÈS SECRET) (SIRC 1999-03)

120. *Proliferation* (TRÈS SECRET) (SIRC 1999-04)

121. *Observations du CSARS sur le projet de loi C-31 dont est actuellement saisi le Parlement* (PROTÉGÉ)* (SIRC 1999-05)

122. *Domestic Targets* (TRÈS SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TRÈS SECRET) (SIRC 1999-07)

124. *Regional Audit* (TRÈS SECRET) (SIRC 1999-08)

125. *Foreign State Activities* (TRÈS SECRET) (SIRC 1999-09)

126. *Le Projet Sidewinder* (TRÈS SECRET)* (SIRC 1999-10)

127. *Security Breach* (TRÈS SECRET) (SIRC 1999-11)

128. *Domestic Exchanges of Information 1999-2000* (TRÈS SECRET) (SIRC 2000-01)

129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999-2000* (TRÈS SECRET) (SIRC 2000-02)

130. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 2000-03)

131. *Regional Audit* (TRÈS SECRET) (SIRC 2000-04)

132. *Warrant Review* (TRÈS SECRET) (SIRC 2000-05)

133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999-2000* (TRÈS SECRET) (SIRC 2001-02)

134. *CSIS Investigation of Sunni Islamic Extremism* (TRÈS SECRET) (SIRC 2002-01)

135. *Source Recruitment* (TRÈS SECRET) (SIRC 2001-01)

136. *Collection of Foreign Intelligence* (TRÈS SECRET) (SIRC 2001-05)

137. *Domestic Extremism* (TRÈS SECRET) (SIRC 2001-03)

138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TRÈS SECRET) (SIRC 2001-04)

139. *Warrant Review* (TRÈS SECRET) (SIRC 2001-06)

140. *Rapport spécial sur des allégations concernant une personne* (TRÈS SECRET)*

141. *Audit of Section 16 and Foreign Intelligence Reports* (TRÈS SECRET) (SIRC 2002-02)

142. *Review of the Ahmed Ressam Investigation* (TRÈS SECRET) (SIRC 2002-03)

143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TRÈS SECRET) (SIRC 2002-04)

144. *Regional Audit* (TRÈS SECRET) (SIRC 2002-05)

145. *Rapport spécial (2002-2003) sur des allégations concernant une personne* (TRÈS SECRET)*

146. *Front End Screening Program* (TRÈS SECRET) (SIRC 2003-01)

147. *CSIS Section 12 Operational Activity Outside Canada* (TRÈS SECRET) (SIRC 2003-02)

148. *Review of a Counter-Intelligence Investigation* (TRÈS SECRET) (SIRC 2003-03)

149. *Review of a Counter-Proliferation Investigation* (TRÈS SECRET) (SIRC 2003-04)

150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TRÈS SECRET) (SIRC 2003-05)

151. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TRÈS SECRET) (SIRC 2004-01)

152. *Review of CSIS's Investigation of Transnational Criminal Activity* (TRÈS SECRET) (SIRC 2004-02)

153. *Review of the Terrorist Entity Listing Process* (SECRET) (SIRC 2004-03)

154. *Review of Activities and Investigations in a CSIS Regional Office* (TRÈS SECRET) (SIRC 2004-04)

155. *Review of a Counter Terrorism-Investigation* (TRÈS SECRET) (SIRC 2004-05)

156. *Review of a Counter Intelligence-Investigation* (TRÈS SECRET) (SIRC 2004-06)

157. *Review of CSIS's Information Operations Centre* (TRÈS SECRET) (SIRC 2004-07)

158. *Review of CSIS's Exchanges of Information with Close Allies* (TRÈS SECRET) (SIRC 2004-08)

159. *Review of a Counter-Proliferation Investigation* (TRÈS SECRET) (SIRC 2004-09)

160. *Terrorist Financing Activities in Canada* (TRÈS SECRET) (SIRC 2004-10)

161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TRÈS SECRET)*

Annexe C

Principales constatations et recommandations

Principales constatations et recommandations

EXAMEN DU PROCESSUS D'INSCRIPTION DES ENTITÉS TERRORISTES

Le CSARS a effectué en 2004-2005 sa première étude d'un rôle que la nouvelle *Loi antiterroriste* du Canada a conféré au SCRS, soit celui que joue le Service dans le processus d'inscription des entités terroristes (IET). Le mandat concernant le processus d'IET est octroyé par l'article 83.05 du *Code criminel* modifié par la *Loi antiterroriste*. Le rôle du SCRS dans ce processus est d'élaborer des rapports de renseignements de sécurité (RRS) dont le ministre de la Sécurité publique et de la Protection civile tient compte au moment de recommander ou non l'inscription d'une entité au gouverneur en conseil.

Le Comité soutient que le processus d'inscription peut obliger le SCRS à recueillir, à conserver et à analyser des informations étrangères à la définition de « menaces envers la sécurité du Canada » selon la *Loi sur le SCRS*. Dans l'ensemble de son étude sur le rôle du Service à l'égard du processus d'IET, il a constaté que la collecte d'informations destinées à ce processus, par le SCRS, avait été conforme aux instructions ministérielles, une fois que celles-ci eurent été données au Service, et aux politiques opérationnelles pertinentes. Le CSARS a néanmoins conclu que le processus obligeait le Service à recueillir certains renseignements qui débordent les pouvoirs énoncés dans la *Loi sur le SCRS*, en ce qui a trait aux « menaces envers la sécurité du Canada ».

Le Comité n'a pu prendre connaissance des RRS lors de son étude du rôle du SCRS dans le processus d'IET du fait qu'il s'agit de renseignements confidentiels du Cabinet. Même si son étude de ce rôle du Service a été assez exhaustive, il n'a néanmoins pu en faire une évaluation complète.

ÉTUDE DE L'ENQUÊTE DU SCRS SUR LA CRIMINALITÉ TRANSNATIONALE

Cette étude visait à évaluer l'enquête du SCRS sur la criminalité transnationale et portait sur les activités menées au Canada par plusieurs organisations criminelles transnationales étrangères. Les enquêtes choisies pour cette étude, de portée nationale, étaient autorisées aux niveaux II et III et concernaient de présumées activités constituant des menaces décrites à l'alinéa 2*b*) de la *Loi sur le SCRS*.

Le Comité a conclu que le SCRS avait raison de croire que les activités de quatre cibles individuelles étaient dirigées par l'étranger ou menées au nom d'intérêts étrangers, et présentaient généralement une menace au sens de la définition de l'alinéa 2*b*) de la *Loi sur le SCRS*. Qui plus est, il a constaté que le Service avait respecté en tous points

les instructions ministérielles et la politique opérationnelle dans ses demandes d'autorisation d'enquête. Le SCRS a en outre pratiqué un degré d'intrusion proportionnel aux menaces présumées.

Cette étude n'a donné lieu à aucune recommandation.

ÉTUDE D'UNE ENQUÊTE ANTITERRORISTE

Cette étude expose les résultats de l'examen d'une enquête antiterroriste du SCRS par le CSARS, dont celui-ci n'avait fait aucune étude exhaustive depuis plus de dix ans et qui demeurait pourtant hautement prioritaire à la Direction de l'antiterrorisme. Cette enquête était l'objet d'une autorisation de niveau III à l'égard de présumées activités constituant des menaces décrites à l'alinéa 2*c*) de la *Loi sur le SCRS*.

Le Comité a choisi pour objet d'une étude approfondie la cible d'une enquête contextuelle, un organisme ciblé, six cibles individuelles, un mandat et six opérations ayant fait appel à des sources humaines. En étudiant des activités opérationnelles clés, il a évalué dans quelle mesure le Service s'était conformé à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Le CSARS a constaté que, d'après les renseignements dont disposait le Service, celui-ci avait des motifs raisonnables de soupçonner les cibles d'enquête autorisées de constituer une menace pour la sécurité du Canada. Le niveau et le degré d'intrusion des enquêtes du SCRS étaient proportionnels à la menace présumée.

Cette étude n'a donné lieu à aucune recommandation.

EXAMEN DES ACTIVITÉS ET ENQUÊTES D'UN BUREAU RÉGIONAL DU SCRS

Chaque année, le Comité s'efforce de faire un examen global des activités du SCRS dans une région particulière. Ce type d'étude englobe le ciblage d'individus, l'exercice de pouvoirs conférés par mandat, le recours à des sources humaines ainsi que la coopération et les échanges d'information avec les partenaires canadiens et étrangers. Le CSARS a aussi examiné les mesures de sécurité interne du SCRS dans la région, ainsi que les manquements et les infractions à la sécurité entre le 1er avril 2000 et le 31 mars 2003.

Dans l'ensemble, les activités de la région en matière d'enquête au cours de la période à l'étude étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle. Le CSARS a constaté que le Service avait des motifs raisonnables de soupçonner les cibles d'enquête autorisées de constituer une menace pour la sécurité du Canada et que le degré d'intrusion des méthodes employées était proportionnel à la menace présumée que constituaient ces cibles.

Au fil de l'étude, l'attention du CSARS a porté sur la participation de certaines cibles à un organisme local qui avait de multiples fonctions. Cela lui a permis de constater que cet organisme avait une double fonction. Le CSARS estime que la politique opérationnelle régissant les enquêtes qui ont ou semblent avoir une incidence sur une fonction devrait s'appliquer à cet organisme. Le SCRS s'est dit en désaccord avec cette constatation.

Le Comité a recommandé que le SCRS définisse un terme particulier de la politique opérationnelle.

ÉTUDE D'UNE ENQUÊTE EN MATIÈRE DE LUTTE CONTRE LA PROLIFÉRATION

Cette étude a porté sur l'enquête menée par le Service à l'égard de la menace que présentaient pour la sécurité du Canada les activités de personnes ou d'organismes liés à un certain pays, entourant la prolifération d'armes de destruction massive.

Le Comité a constaté que le Service s'était conformé en tous points aux instructions ministérielles et à la politique opérationnelle quant aux demandes d'autorisation d'enquête et aux approbations relatives à chacune des enquêtes examinées par le CSARS. Il a conclu que le Service avait des motifs raisonnables de soupçonner chacune des cibles d'enquête autorisées de constituer une menace pour la sécurité du Canada. Le niveau et le degré d'intrusion des enquêtes du SCRS étaient proportionnels à la menace présumée. Celui-ci n'a recueilli que l'information qui lui était strictement nécessaire pour exécuter son mandat.

Le Comité a souscrit à l'approche du SCRS, à savoir engager des entités compétentes du secteur privé à la faveur du Programme de liaison et de sensibilisation. Le Service a rempli toutes les exigences de la *Loi sur le SCRS* et de la politique opérationnelle en ce qui touche l'obtention des mandats. Le CSARS a conclu qu'un bureau régional du Service n'avait pas respecté en tous points les exigences de la politique quant à l'attribution en temps utile, tant verbalement que par écrit, des tâches de l'employé chargé de surveiller l'interception des communications. Le SCRS a respecté les exigences de la politique et les instructions ministérielles en ce qui touche la gestion des opérations examinées, ayant fait appel à des sources humaines. Dans l'ensemble, la coopération et les échanges d'information du Service avec les partenaires canadiens et étrangers étaient conformes à la politique opérationnelle.

Cette étude n'a donné lieu à aucune recommandation.

EXAMEN DU CENTRE DES OPÉRATIONS D'INFORMATION DU SCRS

Le Comité a mené sa toute première étude concernant l'enquête du SCRS sur les menaces aux infrastructures essentielles du Canada en matière d'information, et cela, à deux fins précises. En premier lieu, il a examiné le rôle du Centre des opérations d'information dans les enquêtes sur les menaces contre les infrastructures essentielles du Canada. Puis, le CSARS s'est penché sur les opérations du Centre, vérifiant si une enquête de contre-espionnage au sujet d'une opération informatique était conforme à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle du Service.

Mises à part les deux préoccupations décrites ci-après, le CSARS a constaté que le Service s'était conformé à la *Loi sur le SCRS*, aux instructions ministérielles et à sa politique opérationnelle dans l'exercice de ses fonctions. La première préoccupation du Comité était que la politique opérationnelle aille de pair avec l'affaire examinée.

> **Le CSARS recommande que le Service revoie sa politique opérationnelle pour assurer qu'elle englobe clairement certaines questions relatives aux enquêtes en vertu de l'article 12.**

La deuxième préoccupation du Comité concernait des erreurs administratives.

> **Le CSARS recommande que le Service revoie sa politique opérationnelle pour assurer que, s'il faut renvoyer à des rapports portant un numéro de dossier de la base de données opérationnelles, dans des rapports inscrits sous un autre numéro, cela soit fait dans la partie « Commentaires de l'enquêteur ».**

EXAMEN DES ÉCHANGES D'INFORMATION DU SCRS AVEC LES PROCHES ALLIÉS

L'affaire Arar a braqué l'attention publique sur l'utilisation de l'information qui pouvait avoir été recueillie au Canada, puis communiquée à des partenaires étrangers. Le Comité a décidé de mener son premier examen poussé des échanges d'information du SCRS avec les proches partenaires alliés. À partir de l'une des enquêtes antiterroristes du Service, le Comité a choisi d'en examiner les échanges d'information avec quatre organismes alliés, comme objet premier de son examen détaillé.

Dans le contexte de l'enquête examinée, le CSARS a constaté que les échanges d'information du Service avec les services alliés étaient conformes à l'entente conclue avec chacun d'eux ainsi qu'à la *Loi sur le SCRS*, aux instructions ministérielles et à la

politique opérationnelle. Le Comité a aussi constaté que le Service avait fait preuve de diligence raisonnable en échangeant des informations au sujet des cibles d'enquête.

Le SCRS a obtenu l'approbation requise avant de communiquer les informations aux organismes alliés choisis, mais le CSARS a constaté que la politique opérationnelle devrait indiquer clairement quel niveau de gestion doit rendre compte des échanges d'informations avec des organismes étrangers.

Le CSARS a recommandé que le SCRS modifie la politique opérationnelle afin d'indiquer clairement quel niveau de gestion doit rendre compte des communications aux organismes étrangers.

Dans cette étude, le CSARS a aussi examiné la place qui avait été faite aux droits de la personne dans le contexte des ententes conclues avec des organismes étrangers. Lorsque le SCRS amorce le processus menant à une nouvelle entente avec un organisme étranger, il informe Affaires étrangères Canada et le ministre de la Sécurité publique et de la Protection civile qu'il « scrutera de près la teneur des renseignements fournis à un organisme étranger ou reçus de celui-ci afin d'assurer qu'aucun de ces renseignements ne serve à commettre des actes susceptibles d'être considérés comme des violations de droits de la personne ou n'ait été obtenu par suite de tels actes ». Le Comité a cependant conclu que le SCRS n'était pas en mesure de fournir cette assurance absolue.

Le CSARS a recommandé que le SCRS revoie le contenu des lettres adressées à Affaires étrangères Canada et au ministre de la Sécurité publique et de la Protection civile pour éviter de donner l'impression qu'il peut garantir que l'information fournie à un organisme étranger ou reçue de lui n'a pas servi à commettre des actes susceptibles d'être considérés comme des violations des droits de la personne et n'a pas, non plus, été obtenue par suite de tels actes.

ÉTUDE D'UNE ENQUÊTE DE CONTRE-ESPIONNAGE

L'examen de cette enquête de contre-espionnage par le CSARS a porté sur la période du 1er janvier au 31 décembre 2003. L'objectif était d'évaluer la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles et à toutes les politiques opérationnelles pertinentes.

Dans l'ensemble, l'enquête de contre-espionnage était conforme à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle au cours de la période à l'étude. Le CSARS a constaté que le SCRS avait des motifs raisonnables de soupçonner

les cibles d'enquête autorisées de présenter une menace pour la sécurité du Canada. Il a également constaté que le degré d'intrusion des méthodes employées était proportionnel à la menace présumée que constituaient ces cibles. Les enquêteurs du SCRS ont recueilli uniquement des informations strictement nécessaires à l'enquête. Ils ont aussi agi d'une manière irréprochable et conforme à la loi dans leur recours aux sources humaines.

Tout au long de l'étude, le Comité a porté une attention particulière à l'enquête du Service sur les activités d'ingérence. Il a constaté que les politiques opérationnelles du SCRS visant ces types de situations étaient incomplètes. Aussi a-t-il recommandé que :

> **Le SCRS revoie et modifie, au besoin, ses politiques opérationnelles relatives à des institutions particulières pour assurer qu'elles couvrent tous les aspects d'un processus donné.**

FINANCEMENT DU TERRORISME AU CANADA

L'objectif de cette étude était d'examiner l'enquête du SCRS sur le financement du terrorisme au Canada et d'en faire une étude approfondie. Le Comité a choisi la cible d'une enquête contextuelle et cinq cibles particulières. Dans chaque cas, il a évalué la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le Comité a conclu que le Service avait des motifs raisonnables de soupçonner les activités des individus et groupes ciblés de présenter une menace pour la sécurité du Canada. Le niveau et le degré d'intrusion de l'enquête du SCRS étaient proportionnels à la menace présumée, et celui-ci a recueilli uniquement des informations nécessaires à l'exécution de son mandat. Ses activités étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le CSARS était satisfait du degré et de la nature de la coopération du Service avec ses partenaires canadiens et étrangers.

Il est possible que le Service soit tenu de recueillir et d'analyser des informations concernant une entité qui répond à la définition de *personne ou groupe inscrit* en vertu du *Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme* mais qui ne présente pas une *menace envers la sécurité du Canada*, selon l'article 12 de la *Loi sur le SCRS*. De plus, le Comité a noté que le *Règlement* n'enjoint pas expressément au Service de prendre part au processus d'inscription et que le ministre de la Sécurité publique et de la Protection civile ne lui a pas donné, non plus, d'instruction particulière à cet égard.

Cette étude n'a donné lieu à aucune recommandation.

LIAISON DU SCRS AVEC DES ORGANISMES ÉTRANGERS : EXAMEN D'UN BUREAU DE LIAISON-SÉCURITÉ

Le Comité a cherché à déterminer si les échanges d'information de ce bureau de liaison-sécurité avec des organismes étrangers respectaient la portée des ententes de liaison existantes, approuvées par le gouvernement. Il en a aussi évalué les opérations par rapport à la *Loi sur le SCRS* et aux instructions ministérielles ainsi qu'aux politiques et procédures opérationnelles du Service.

Pour se mettre en contexte, le Comité a aussi examiné les opérations de ce bureau et les a évaluées par rapport aux questions qu'il pose lors de l'examen suivi des ententes du SCRS avec des organismes étrangers, en vertu de la loi. De plus, dans son rapport, le CSARS a tenu compte des tendances observées dans ses études des cinq dernières années sur les agents de liaison-sécurité.

Le manque de documents du Service qui aient été mis à jour, pour évaluer les rapports de liaison de ce bureau, a suscité certaines préoccupations au Comité. En dépit des directives écrites concernant l'élaboration et la mise à jour de tels documents, le SCRS n'a pas de politique officielle à cet égard. Le CSARS a formulé la recommandation suivante :

> **Le Comité a recommandé que le Service instaure des politiques pour l'élaboration, la mise à jour et la présentation annuelle de ses documents qui servent à évaluer la portée des échanges avec des organismes étrangers.**

EXAMEN DES ENTENTES AVEC DES ORGANISMES ÉTRANGERS

En vertu du paragraphe 17(1) de la *Loi sur le SCRS*, le Service peut conclure une entente avec le gouvernement d'un État étranger, ou avec une organisation internationale d'États (ou avec ses institutions), dans le but d'exercer ses fonctions. En vertu du sous-alinéa 38*a*)(iii) de la *Loi*, le Comité est tenu d'examiner toutes ces ententes. Au cours de 2004-2005, le Comité a réalisé sa première étude approfondie du processus d'élargissement d'ententes. Il y a amélioration ou élargissement d'une entente existante lorsque le Service la modifie. Cela définit la teneur et l'ampleur des échanges autorisés.

Le CSARS a constaté que le SCRS s'était conformé aux conditions énoncées dans les instructions ministérielles et dans la politique opérationnelle à l'égard de l'élargissement des dix ententes existantes, conclues avec des organismes étrangers. Au sujet des autorisations d'élargissement, le Comité a noté que le Service n'avait pas de politique opérationnelle quant au type d'informations à inclure dans la demande au directeur. Il a aussi noté que les évaluations des organismes avec lesquels le SCRS a des ententes n'étaient pas toujours présentées chaque année, tel que prescrit dans le Manuel des procédures pour les postes de la Liaison avec l'étranger.

Cette étude n'a donné lieu à aucune recommandation.